Controlled Substance Ordering System (CSOS)

Certification Practice Statement (CPS)

Prepared for

Drug Enforcement Administration
Office of Diversion Control
E-Commerce Program (ODC)
Washington, DC 22202

Public Version 2.1

January 31, 2006

Prepared by
Nortel Government Solutions, Inc.

Document Revision History

Change #	Revision Date	Sections/Pages Affected	Summary of Changes	Initials
1	August 18, 2005	4.1	Changed “digitally-signed email” to “email” to mitigate client S/MIME handling issues.	ML
2	August 30, 2005	All Pages	Added FOUO statement to all footers	ML
3	August 30, 2005	Section 4.6.4 – Protection of Archive	Clarified paragraph. Differential backups are not archived.	ML
4	August 30, 2005	Various	Removed backup and archive media type specifics so that backup media types could be replaced with newer technologies as appropriate.	ML
5	August 30, 2005	Section 3.1.1	Reworded section per DEA clarification, as there may be cases where importers are also distributors and would be both Subscribers and Relying Parties – although not to their own Registration’s transactions.	ML
6	September 8, 2005	Modified exhibits 4-3 and 5-3	Added revocation reason to exhibit 4.3 for CA Administrative Action (Superseded) to accommodate revocation due to technical reasons. Modified 5-3 to specify generic tools.	ML
7	October 31, 2005	2.5, 2.6.3, 3.1.11.4, 3.2.1, 3.2.2, 3.3, 3.4, 4.1, 4.4.1.1, 4.4.3, 4.4.3, 4.4.6, 4.4.7, 4.4.9.1, 4.5.4, 4.8.1, 5.2.1.6, 6.1.5, 6.2.3,	Modified verbiage to represent new processes and to clarify sections per auditor’s review.	ML
8	Nov 2, 2005	3.3 – Rekey after Revocation	Modified verbiage to accommodate revocation circumstances due to technical malfunctions.	ML
9	January 26, 2006	3.1.10, 3.1.11.4, 4.6.5, 6.3.2, 5.1.4.3	Modified verbiage to accommodate FBCA cross-certification and KPMG comments.	ML
10.	March 7, 2006	All	Technical edit	JT

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Section 1 – Introduction

1.1 Overview

A Certification Practice Statement (CPS) is a statement of the practices that a Certification Authority employs when issuing certificates. This CPS establishes the procedures that satisfy the DEA Diversion Control E-Commerce System Certificate Policy (CP) for the management of certificates within a Certification Authority domain, stating the operating procedures for the Certification Authority and clarifying legal rights and obligations.

This *Controlled Substance Ordering System (CSOS) Certification Practice Statement* (henceforth referred to as CPS) has been developed in accordance with recommendations contained in Internet Engineering Task Force (IETF) Request for Comment (RFC) 2527.

The CSOS Certification Authority (CA) is an entity established to create, sign, and issue public key certificates to authorized CSOS Subscribers through subordination to the DEA Diversion Control E-Commerce Bridge CA. The CSOS CA is subordinate to the DEA Diversion Control E-Commerce Bridge CA, which functions as the Root CA for CSOS CA. The terms DEA Diversion Control E-Commerce Root CA (or, "Root CA" and the DEA Diversion Control E-Commerce Bridge CA ("DEA Bridge CA") are synonymous and will be used as appropriate within the text of this document.

This CPS describes the practices of the CSOS CA in issuing and otherwise managing CSOS certificates issued to DEA Registrants, CSOS Coordinators, and holders of Powers of Attorney (POAs). It provides the details for the certification process. This CPS also describes the process for suspending, revoking, and renewing certificates. The scope of this document is applicable to the CSOS Public Key Infrastructure (PKI). Future updates to this document are planned to accommodate DEA Bridge CA activities supporting DEA's Electronic Prescriptions for Controlled Substances (EPCS) initiative. Due to the sensitive nature of the security controls described within this document, this document is not made publicly available in its entirety. Requests for the complete CPS may be made by authorized parties to the PMA at the address cited in section 1.4.2.

This CPS describes:

- The mechanisms that will be used to authenticate the identity of all individuals who need to interact with the CSOS PKI.
- The methods used to ensure the integrity of all information that is communicated.
- The format(s) of the input certification requests.

- The algorithms(s) used for signing the hashed content summary of the certificate request that are accepted by the CSOS CA and the algorithms used by the CSOS CA to sign the certificates that it generates.
- The validity period of the certificates issued by the CSOS CA.
- The procedures for renewing certificates.
- The technical procedures for revoking certificates generated by the CSOS CA.
- The backup procedures that will ensure that all data is recoverable in case of failure.
- The methods of protecting sensitive information from unauthorized access.
- The methods of distributing and accessing the certificates generated by the CSOS CA.

1.2 Identification

This document serves as the CSOS CPS. The practices stated herein conform to and support the DEA Diversion Control E-Commerce System Certificate Policy, version 2.0, dated April 29, 2005, that is registered with the National Institute of Standards and Technology (NIST) and identified by the assigned object identifier (OID) dea-csos-cp ::= { 2.16.840.1.101.3.2.1.9.1}. All certificates issued to CSOS Subscribers by the CSOS CA will carry this OID. Administrative and component certificates used for device or service signing or encryption, issued by the CSOS CA, will not carry this OID.

Only the CSOS CA that is designated and managed by the DEA or its contractor, Nortel Government Solutions, Inc.,, is authorized to issue CSOS Subscriber certificates. The CSOS CA will not fully cross-certify with other CAs. It is anticipated the DEA Bridge CA will establish a one-way cross-certification with the Federal Bridge CA to enable Relying Parties to accept CSOS Subscriber certificates for purposes other than controlled substance orders.

1.3 Community and Applicability

This CPS identifies the specific privileges and the specific restrictions assigned to CSOS CA participants and the mechanisms by which these attributes are granted and enforced. This includes individuals involved in both implementing the CP, CPS, and managing the CSOS PKI. This CPS contains information sensitive to the security of the CSOS PKI and will therefore not be released in its entirety to the public without the express permission of the DEA Diversion Control E-Commerce Section Chief or Policy Management Authority Chair.

1.3.1 Policy Management Authority (PMA)

The DEA Diversion Control E-Commerce System Policy Management Authority (PMA) is the governing body responsible for the DEA Diversion Control E-Commerce System initiatives. The mission of the PMA is to establish, interpret, and enforce policy for the DEA Bridge CA and

the CSOS CA in accordance with all applicable US laws and regulations. The PMA approves the CP and CPS for the DEA Diversion Control E-Commerce System and also approves all changes to the document as discussed in Section 8 of this CPS. Operational tasks for which the PMA has oversight responsibility are delegated to the Operations Management Authority (OMA).

The PMA is run as a formal committee. PMA membership consists of selected individuals working within DEA Office of Diversion Control, E-Commerce Section (ODC), Liaison and Policy Section (ODL), Registration and Program Support section (ODR), the DEA Diversion Control PKI Operations Management Authority (OMA), the DEA CIO or his or her representative and the Contracting Officer's Technical Representative (COTR) supervising contractor activities relating to the DEA Diversion Control E-Commerce System.

The official list of PMA members will be maintained at the DEA Diversion Control E-Commerce System Web site at: http://www.DEAecom.gov. PMA obligations are discussed in Section 2.1.1.

1.3.2 Operations Management Authority (OMA)

The OMA is responsible for the daily operation and maintenance of the DEA Electronic Commerce PKI systems (both CSOS and EPCS operations). The OMA consists of the DEA Diversion Control E-Commerce Section Chief, the Operations Manager and his staff, and the Sr. Policy Manager and Systems Engineering Manager. The DEA Diversion Control E-Commerce Section Chief provides planning guidance and direction to this team and, in turn, presents operational status and issues to the PMA for consideration.

1.3.3 DEA Diversion Control E-Commerce System Bridge CA (DEA Bridge CA)

The DEA Bridge CA is operated and maintained by Nortel Government Solutions, Inc., under the authority of the DEA. The DEA Bridge CA serves as the Root CA to the CSOS CA, issuing and signing public key certificates for the CSOS CA. The DEA Bridge CA will additionally issue subordinate certificates and cross-certificates to other CAs that participate in the Electronic Prescription Ordering System (EPCS). DEA Bridge CA obligations are discussed in Section 2.1.3.

1.3.4 CSOS Subordinate Certification Authority (CSOS CA)

The CSOS CA is an entity established and authorized by the PMA to create, sign, and issue public key certificates to authorized CSOS Subscribers through subordination to the DEA Bridge CA. The CSOS CA is operated and maintained by Nortel Government Solutions, Inc., under the authority of the DEA. A description of the implementation may be found in Section 5 of this document. The CSOS CA issues and manages CSOS Subscriber certificates and Certificate Revocation Lists (CRLs) in accordance with the terms and conditions specified within the most recent version of the CP. CSOS CA obligations are discussed in Section 2.

1.3.5 Registration Authority (RA)

The CSOS CA performs both the role and the functions of a Registration Authority (RA). The RA processes applications of CSOS Coordinators and Subscribers according to the stipulations of the Certificate Policy. The RA function includes both automated and manual processes performed by the CSOS CA registrar. In this CPS, the term *Registrar* is used to refer to an individual performing RA functions, while RA is used to refer to the total RA entity, including the software and its operations. Functions performed by the RA include:

- The verification and authentication of individuals or entities who are designated CSOS Coordinators;
- The approval or rejection of certificate applications;
- The initiation and authentication of certificate revocations; and
- The authentication of individuals or entities submitting requests to renew certificates or seeking a new certificate following revocation.

The following documents detail the RA's responsibilities and tasks specific to CSOS enrollment, adjudication and revocation processes:

- *CSOS Subscriber Manual* located at www.DEAecom.gov.

1.3.6 CSOS Coordinator

Each participating organization must designate Principal and Alternate CSOS Coordinators for each of its DEA registered locations. These CSOS Coordinators serve as the Local Registration Authority (LRA) for the DEA Registrations identified on their applications and are responsible for verifying the identity and applicability of organization personnel applying for a CSOS Certificate. CSOS Coordinators not possessing ordering authority receive administrative certificates for identification purposes when communicating electronically with the RA. The *Registrant Agreement* and the *CSOS Subscriber Manual* documents located at www.DEAecom.gov detail the CSOS Coordinator's responsibilities. CSOS Coordinator obligations are discussed in Section 2.1.6.

1.3.7 Subscribers (all who transmit electronic orders)

A Subscriber is the entity whose name appears as the subject in a certificate issued by the CSOS CA, who attests that it uses its key and certificate in accordance with the Certificate Policy asserted in the certificate. DEA registrants are those entities required under the Federal Controlled Substances Act (CSA) to register with DEA. According to the CSA, a separate registration is required for each principal place of business or professional practice at one general physical location where controlled substances are manufactured, distributed, imported, exported, or dispensed by a person (21 U.S.C. 822(e)). Distributors, manufacturers, importers, and exporters of controlled substances fall into this category of DEA registrant. Other registrants

include individual practitioners such as doctors, dentists, nurses, veterinarians, and other medical personnel who are not "an agent or employee of any registered manufacturer, distributor, or dispenser of any controlled substance or list I chemical."

There are various classes of DEA registrants: manufacturers, distributors, dispensers/ practitioners (which includes hospitals, clinics, retail pharmacies, and teaching institutions), researchers, narcotic treatment programs, importers, exporters, and chemists. When the designation "registrant" refers only to an approved company location, that company must designate legal Powers of Attorney (POAs) the responsibility for ordering controlled substances on that company's behalf. CSOS Subscriber certificates are issued only by the CSOS CA and are limited to approved DEA Registrants and the company's holders of Powers of Attorney (POAs).

The CSOS CA will limit the issuance of special purpose or administrative certificates to CSOS Principal and Alternate Coordinators, DEA employees, authorized Department of Justice (DOJ) officials, and properly cleared and approved contractor personnel. The *Subscriber Agreement* and *CSOS Subscriber's Manual* documents located at www.DEAecom.gov provide enrollment instructions. Subscriber obligations are discussed in Section 2.1.7 of this CPS.

1.3.8 Relying Parties (all who accept electronic orders)

A Relying Party is the entity that, by using a Subscriber's certificate to verify the integrity of a digitally signed message, identifies the creator of a message and relies on the validity of the public key bound to the Subscriber's name. The Relying Party is responsible for checking the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message and to identify the creator of a transaction. Replying Party obligations are discussed in Section 2.1.8 of this CPS.

1.3.9 Applicability

CSOS Subscriber certificates are only issued to entities engaged in the transfer of controlled substances between manufacturers, distributors, retail pharmacies, authorizing institutions and other registrants and must be used for the signing of electronic transaction orders, however the use of CSOS certificates is not restricted to this single application. CSOS certificates may not be used for the signing of electronically transmitted controlled substance prescriptions. The practices described in this CPS apply to the issuance and use of those certificates, Authority Revocation Lists (ARL) and Certificate Revocation Lists (CRL) for users within the CSOS CA domain.

1.4 Contact Details

1.4.1 Specification Administration Organization

The DEA, Office of Diversion Control, is the administering organization for this CPS.

1.4.2 Contact Person

The contact details for the DEA Diversion Control E-Commerce System Certificate Policy, Version 2, dated April 29, 2005, and this CSOS Certification Practice Statement, Version 1.0 dated February 15, 2005 and PKI are located at www.DEAecom.gov. Written communication should be sent to:

Drug Enforcement Administration
Office of Diversion Control
E-Commerce Program (ODC)
Attn: Chair, Policy Management Authority
Washington, DC 22202

1.4.3 Person Determining CPS Suitability for the Policy

The DEA Diversion Control E-Commerce System PMA is responsible for determining the suitability of this CPS and of the DEA Diversion Control E-Commerce System. The PMA is responsible for the approval of the CP, approval of all Subscriber agreements, and the review and approval of this CPS to ensure its consistency with the CP. The CSOS CA will be required to periodically attest to the compliance of the CPS to the CP as set forth in the CP.

Section 2 – General Provisions

2.1 Obligations

2.1.1 PMA Obligations

PMA obligations are listed below:

- The PMA is responsible for review and approval of this CPS, and provides approval authority for subsequent changes to this CPS, to ensure its consistency with the CP.
- The PMA is responsible for the approval of all Subscriber agreements.
- The PMA is ultimately responsible for resolution of any name claim disputes.
- The PMA will approve any fees levied by the OMA.
- The PMA establishes the qualifications for the selection of entities seeking to perform a compliance audit.
- The PMA will review compliance audits for the CSOS CA and any cross-certified or subordinate EPCS CAs and make appropriate determinations.
- The PMA will ensure that CSA database information is readily available for verification.
- The PMA will evaluate (or direct the evaluation of) applicant CAs seeking EPCS cross-certification or subordination to the DEA Bridge CA.

2.1.2 OMA Obligations

The OMA is responsible for daily operations of the DEA Diversion Control E-Commerce System and for the development and maintenance of operations and policy documents. Operational roles, responsibilities and procedures are maintained in operations guides made available to staff in the DEA PKI facility.

2.1.3 DEA Diversion Control E-Commerce System Bridge CA (DEA Bridge CA)

DEA Bridge CA executes the following obligations in accordance with the CP:

- Provides a copy of its CPS to the PMA, as well as any subsequent changes, for approval and conformance assessment;
- Protects the private signing key of the DEA Bridge CA in accordance with the CP and this CPS;

- Issues and manages certificates to the CSOS CA.

- Signs certificates only after verifying the identity of the certificate subject in accordance with the CP and this CPS, and that the subject holds the private key corresponding to the public key in the certificate;

- Uses the private signing key only when issuing certificates or signing Authority Revocation Lists (ARLs) which conform to the CP and this CPS;

- Operates a repository for maintaining CA certificate information and status, publishing information to the repository consistent with this CPS;

- Revokes the CSOS CA certificate if the CSOS CA is found to have acted in a manner counter to those obligations to which it agreed to conform;

- Provides for CSOS CA certificate updating or re-keying.

2.1.4 CSOS CA Obligations

The CSOS CA complies with the provisions defined in the DEA Diversion Control E-Commerce System CP, by following the procedures outlined in this CPS. Obligations include the following:

- Provides this CSOS CPS to the PMA, as well as any subsequent changes to the CPS, for conformance assessment in accordance with Section 8 of this CPS.

- Protects the CA's private signing key in accordance with Section 5.2 of this CPS;

- Signs certificates only after verifying the identify of the certificate subject in accordance with Section 3.1.11 of this CPS;

- Verifies that the subject holds the private key corresponding to the public key in the certificate in accordance with Section 3.1.9 of this CPS;

- Uses the private signing key only when issuing certificates or signing Certificate Revocation Lists (CRL);

- Accepts registration information only from enrolled CSOS Coordinators as described in Section 3.11.1 of this CPS,

- Includes only valid and appropriate information in the certificate in accordance with Section 7.1 of this CPS,

- Maintains evidence that due diligence was exercised in validating the information contained in the certificate in accordance with Sections 4.1 and 4.2.1 of this CPS;

- Ensures that Subscribers are informed of their obligations and informed of the consequences of not complying with those obligations in a Subscriber Agreement and by requiring acceptance of these obligations and terms as a condition of certificate retrieval as specified in Section 3.1 of this CPS.

- Revokes the certificates of Subscribers found to have acted in a manner counter to those obligations as specified in Sections 4.3, 4.4, and 4.4.1.1 of this CPS;

- Provides for certificate updating or re-keying as specified in Section 3.2.1 of this CPS;

- Operates or provides for the service of a repository for maintaining Subscriber certificate information and status as specified in Section 2.6.4 of this CPS;

- Maintains records necessary to support requests concerning its operation, including audit files and archives as specified in Sections 2.6.4 and 4.6 of this CPS;

- Accurately publishes CRLs, process certificate applications and respond to revocation requests in a timely and secure manner as specified in Section 4.4.9.1 of this CPS.

2.1.5 RA Obligations

The CSOS RA is responsible for controlling the registration process through the adjudication of applications received from CSOS Coordinators and Subscribers, collecting and verifying the information to be entered into the certificates issued by the CSOS CA. In the performance of these duties, the CSOS RA is obligated to:

- Verify the accuracy and authenticity of the Subscriber information at the time of application for a certificate.

- Validate and process Subscriber certificate revocation requests in accordance with the stipulations of the CP and this CPS.

- Provide the CSOS CA with the necessary information to complete the certificate issuance and revocation processes.

2.1.6 CSOS Coordinator Obligations

For individuals applying for a CSOS certificate associated with a DEA registered location for which the CSOS Coordinator is responsible, the CSOS Coordinators:

- Verify the applicant’s identity and employment;

- Verify that the applicant’s CSOS application packet has been properly completed and signed by the applicant;

- Submit the signed application packet to the CSOS Registration Authority;
- Maintain evidence that due diligence was exercised in validating the information contained in the Subscriber's application;
- Serve as a point of contact for CSOS notification for their registered location, supplying confirmation of certificate requests, certificate renewals, and revocation requests.

2.1.7 Subscribers Obligations

CSOS Subscribers are obligated to adhere to the regulations specified in 21 U.S.C. 1300-end and the responsibilities specified in the Subscriber Agreement (available at www.DEAecom.gov).

2.1.8 Relying Party Obligations

Relying Parties that accept orders for controlled substances are obligated to adhere to the regulations specified in 21 U.S.C. 1300-end.

2.1.9 Repository Obligations

The OMA operates and utilizes a variety of mechanisms as required by the CP to ensure that there is a repository where the CSOS CA certificate and CRLs are published. The mechanisms supported and operated include:

- An X.500 compliant Directory Service System with Lightweight Directory Access Protocol (LDAP) V3 access that allows authorized access and retrieval of the Certificate Revocation Lists and the CSOS CA certificate information.
- A CSOS Web site is maintained at www.DEAecom.gov for posting CSOS public documentation including the CP, Subscriber Manual and other public documentation as appropriate. Access controls are implemented to ensure that the modifications to these documents are limited to authorized personnel only.
- The CA has implemented administrative access controls to protect the repository information from unauthorized access. The controls are enforced through application configuration and operating system and procedural controls that ensure accountability.
- The CA has implemented system and environmental controls to ensure that a high level of reliability and availability is provided to the using community.

2.2 Liability

The U.S. Government shall not be liable to any party, except as determined pursuant to the Federal Tort Claims Act (FTCA), 28 U.S.C. 2671-2680, or as determined through a valid express written contract between the Government and another party.

2.3 Financial Responsibility

The U.S. Government shall bear no financial responsibility, except as determined pursuant to the Federal Tort Claims Act (FTCA), 28 U.S.C. 2671-2680, or as determined through a valid express written contract between the Government and another party.

2.3.1 Indemnification by Relying Parties and Subscribers

The PMA, DEA Bridge CA, and CSOS CA assume no financial responsibility for improperly used certificates.

2.3.2 Fiduciary Relationships

Issuance of certificates in accordance with this CP shall not make the DEA Bridge CA an agent, fiduciary, trustee, or other representative of the subordinate or cross-certified CAs or their Subscribers.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

U.S. Government laws will govern the enforceability, construction, interpretation, and validity of this CPS.

2.4.2 Severability, Survival, Merger Notice

Should it be determined that one section of this CPS is incorrect or invalid, the other sections will remain in effect until the document is updated. Requirements for updating this CPS are described in Section 8.

2.4.3 Dispute Resolution Procedures

Disputes are submitted in writing to the PMA Chair for resolution. The PMA Chair will make the determination on whether an out-of-cycle PMA meeting should be held to address the dispute, or whether the dispute will be added to the agenda at the next regularly scheduled PMA meeting. Prior to the meeting in which the dispute will be addressed, the Chair should ensure that all voting members have received notification and information regarding the matter in dispute. Any PMA voting member may request to have the parties involved attend the meeting to provide more discussion. Every attempt should be made to resolve the dispute by negotiation, however

the PMA will have the sole authority for the resolution of any disputes by quorum vote of the membership.

2.5 Fees

DEA does not charge fees for the issuance of CSOS Subscriber certificates or to status checking information (CRLs), nor will the CA impose any fees to end entities for the reading of the Certificate Policy, this CPS, or any other document incorporated by reference.

The OMA, with the approval of the PMA, will determine the fees, if any, for other CSOS services. The OMA reserves the right to charge fees for the issuance of certificates as well as for access to certificate status information, subject to agreement between the CA and the Subscriber and/or between the CA and the Relying Party, in accordance with a fee schedule that would, at that time, be posted onto the CSOS web site.

2.6 Publication and Repositories

2.6.1 Publication of CA Information

The following PKI information is published in the CSOS repository:

- Certificate revocation information for all CSOS certificates that the CA issues;
- The DEA Bridge CA's self-signed CA certificate containing the public key, which is used to verify the authenticity of the CSOS CA certificate;
- The CSOS CA certificate signed by the DEA Bridge CA containing the public key, which is used to verify the authenticity of a CSOS certificate.

In order to mitigate the risk of aggregated information contributing to the possibility of the diversion of controlled substances, Subscriber certificates are not posted into the CSOS repository.

The following CSOS PKI information will be published on the Web site at www.DEAecom.gov:

- A copy of the DEA Diversion Control E-Commerce System CP;
- A copy of the Subscriber Agreement;
- A copy of the Registrant Agreement;
- The CSOS DEA Registrant Certificate Application Checklist;
- Certificate application forms and instructions;
- Revocation request procedures;

- CSOS Certificate Profile and CSOS Certificate and CRL Profile and Addendum
- The official list of PMA members;
- Contact details for this CPS and PKI;
- A copy of the CSOS Subscriber Manual.

2.6.2 Frequency of Publication

CRLs issued by the CA are automatically published in the directory as soon as they are issued. The frequency of CRL issuance is discussed in Section 4.4.8.1 of this CPS.

2.6.3 Access Controls

The following represents a sanitized description of the access controls in place. Information representing "critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities" has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.

The CSOS Web site enables read-only access to the CP and other public documents contained in the site to Internet users. Only authorized CA personnel are able to modify or post documents on the CSOS web site.

The CSOS CA public repository resides behind a firewall. Public access to the border directories is limited to read access to the CRL and certificate information stored within this repository. The application is configured so that only authenticated directory updates are published. The procedures for issuing Subscriber certificates require multi-person access controls. CSOS Subscriber certificates are not published in this public repository and the directories are protected against unauthorized modification.

2.6.4 Repositories

An X.500 directory provides the public repository for this CA in the external network. Access to the directory is provided through an interoperable implementation of the Lightweight Directory Access Protocol (LDAP) version 3. A web site is also provided to publish CSOS documentation. Repository URLs are listed below:

Purpose	Uniform Resource Locator (URL)
X.500 LDAP V2 or later Directory	Text removed. Information representing "critical infrastructure that could be used to develop an

	attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities" has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.
DEA Diversion Control E-Commerce System CP	http://www.deaecom.gov
CSOS Subscriber Manual	http://www.deaecom.gov

Exhibit 2–1. Repository URLs

2.7 Compliance Audit

2.7.1 Frequency of Entity Compliance Audit

The OMA will arrange full and formal initial and annual audits to validate that the PKI is operating in accordance with the security practices and procedures described in this CPS. Results of the audits are provided to the PMA.

The PMA may order a compliance audit or inspection at any time of the CSOS CA, RA or any Local RA services being provided by CSOS Coordinators in order to validate that these entities are operating in accordance with the security practices and procedures described in the CPS.

2.7.2 Identity/Qualifications of Auditor

Auditors are selected through competitive bidding processes. The PMA establishes the qualifications for the selection of entities seeking to perform a compliance audit. Selected auditors are qualified to perform an American Institute of Certified Public Accountants (AICPA) audit to the WebTrust Principles and Criteria for Certification Authorities ("CA Trust") and perform system audits as their primary responsibility.

Selected auditors are provided with copies of the policy documents and security plans in order to familiarize themselves with the requirements that the PMA imposes on the issuance and management of the CSOS certificates as provided in the CP prior to conducting the audit.

KPMG has been selected to conduct the audit and will validate through document reviews, personnel interviews, and demonstrations that the DEA E-Commerce System is in compliance with its CP.

2.7.3 Auditor's Relationship to Audited Party

The compliance auditor is a contractor that is sufficiently independent from the DEA, PMA or OMA to provide an unbiased, independent, and repeatable evaluation.

2.7.4 Topics Covered by Audit

Compliance audits will use the American Institute of Certified Public Accountants (AICPA) WebTrust for Certificate Authorities criteria and will adhere to the scope established by the PMA. The audit will investigate all aspects of the CA operations to ensure compliance with this CPS, the CP and other CA security policies and procedures. The AICPA/CICA WebTrust Program for Certification Authorities is consistent with standards being developed by the American National Standards Institute (ANSI) and the Internet Engineering Task Force (IETF). *The WebTrust for Certification Authority Principles and Criteria* can be found http://www.webtrust.org/CertAuth_fin.htm.

2.7.5 Actions Taken as a Result of Deficiency

Should the compliance auditor find a discrepancy between the CA's operation and the stipulations contained in the CP or CPS, the following must occur:

- The compliance auditor will note the discrepancy;
- The CA will provide written notification of the audit results to the PMA and OMA, specifically identifying any deficiencies noted as a result of the compliance audit, within 3 business days;

- Once notified, the PMA and OMA will have 10 business days to review the results and the recommendations from the compliance audit to determine the action to be taken.
  - Based on the findings of the compliance audit, appropriate remedies may include:
    - Warn the CA in writing and specify a time period during which the discrepancy must be resolved;
    - Immediately suspend the CA's authority to issue new certificates.

    Several factors must be considered in this decision, including the severity of the discrepancy and the risks it imposes, and the disruption to the certificate-using community;
  - The implementation of proposed remedies, including a time for their completion, will be communicated in a written report to the PMA.

Upon correction of the discrepancy, the CA may request reauthorization. A special audit may be required to confirm the implementation and effectiveness of the remedy.

2.7.6 Communication of Results

Notification of compliance audit failure, the topics of failure, reasons for failure, and possible remedies will be provided within 24 hours, upon the conclusion of the compliance audit, in a written form (signed e-mail or letter) to the PMA and OMA. A full, written, notification of the audit results will be provided to the PMA and the OMA within 3 business days. The report will contain a summary table of topics covered, areas in which the CSOS CA was found to be non-compliant, a brief description of the problem(s) for each area of non-compliance, a brief description of the problem(s) for each area of non-compliance, and possible remedies for each area. The report will also contain the detailed results of the compliance audit for all topics covered, including the topics in which the CSOS CA passed and the topics in which the CSOS CA failed.

In the case of a deficiency action, the PMA will make an effort, as they deem appropriate, to ensure that all CSOS PKI Subscribers are informed of the action. Communication to users to inform them of any deficiency and action is performed via email if possible through the CSOS Coordinators. If a CSOS Coordinator does not have e-mail access, then a letter will be sent to the Subscriber.

2.8 Confidentiality

All information that is not included in the certificates will be protected and access will be restricted as defined in the following subsections.

2.8.1 Types of Information to be Kept Confidential

Each Subscriber’s private signing key is private to that Subscriber. The CA and RA are not provided any access to these keys.

Information held in CA audit trails will be considered confidential to the DEA and will not be released outside the organization, unless required by law.

Personal and agency information held by the CA, other than that which is explicitly published as part of a certificate, CRL, CP or this CPS is considered private and will not be released outside the DEA, unless required by law. The Subscriber information will be used only for the purpose collected and such information will not be released without the prior written consent of the Subscriber, unless otherwise required by law. The results of audits will be kept confidential, with exceptions as deemed appropriate by the PMA.

2.8.2 Information Release Circumstances

Subscriber information from this system may be disclosed to the following parties:

- To federal, state or local agencies along with state medical and licensing boards responsible for investigating, prosecuting, enforcing, or carrying out a statute, rule, regulation, or order when the DEA Office of Diversion Control becomes aware of a violation or potential violation of civil or criminal law or regulation.
- To a member of Congress or to a congressional staff member in response to a request from the person who is the subject of the record.
- To a DEA employee, an expert consultant, or contractor of DEA in the performance of a federal duty to which the information is relevant.
- Persons registered under the Controlled Substances Act (P.L. 91-513) for the purpose of verifying the registration of customers and practitioners.

Unless otherwise required by law and under the conditions stated above, Subscriber information will be used only for the purpose collected and agreed and such information will not be released without the prior written consent of the Subscriber. Any request for release of Subscriber information will be authenticated. The authentication will consist of validating the identity of the requester using two forms of photo identification. In the case where a Subscriber's information is provided to a third party – the third party's authority to obtain the information will be validated using at least one of the following means:

- The individual has the duly executed court order from a Federal court;
- The individual has a duly executed request from the respective Agency Office of Inspector General.

Information that may be reviewed includes only that information pertaining to the individual subscriber submitting the request that is maintained by the DEA in a system of records.

Detailed instructions for making requests for access to records are provided on the CSOS Web site. In response to a proper request for access, CSOS will notify the requesting individual subscriber whether the CSOS system of records contains any records pertaining to him or her, and, if records exist, the manner in which those records may be reviewed.

2.8.3 Types of Information Not Considered Confidential

Information included in the CP, public certificates, and CRLs issued by the CSOS CA is not considered confidential.

2.8.4 Disclosure of Certificate Revocation/Suspension Information

When the CA revokes a certificate, a revocation reason will be included in the CRL entry for the revoked certificate. This revocation reason code is not considered private and can be shared with all other users and relying parties. However, no other details concerning the reason for revocation will be disclosed.

2.8.5 Release to Law Enforcement Officials

Information released to law enforcement officials will be in accordance with applicable laws and regulations. Any request for release of Subscriber information will be authenticated. The authentication will consist of validating the identity of the requester using two forms of photo identification.

2.9 Intellectual Property Rights

Subscriber private signature keys will be treated as the sole property of the legitimate holder of the corresponding public key identified in a CSOS certificate.

Certificates and CRLs issued by the DEA Bridge CA and CSOS CA are the exclusive property of the U.S. Government.

The CP, this CPS, and CSOS Object Identifiers (OID) are the exclusive property of the U.S. Government.

Section 3 – Identification and Authentication

3.1 Initial Registration

Separate application processes are established for the identification of CSOS Coordinators and Subscriber applications and are discussed below.

3.1.1 CSOS Coordinator Registration

While it is not required that a CSOS Coordinator be a DEA Registrant or have been provided POA to order controlled substances for the Registrant, DEA Registrants and POAs may serve as either CSOS Coordinators or Subscribers, and, in some instances, may be both the CSOS Coordinator and Subscriber. As CSOS Coordinators largely consist of regulatory personnel assigned by DEA Registrants and Relying Parties in CSOS are generally comprised of suppliers and manufacturers, it is not anticipated that a business model would arise that would result in a CSOS Subscriber/POA additionally serving in a role as a Relying Party to a transaction signed using a CSOS Subscriber certificate issued to their own DEA Registration.

Applications are identified on the DEA Web site and instructions are provided to walk the applicant through the registration process. To be designated a CSOS Coordinator an applicant must:

(i) Complete and submit a signed, notarized CSOS Coordinator application to the CSOS RA, providing all information requested by the CSOS RA without any errors, misrepresentation, or omissions. Send the notarized application to the CSOS Registration Authority at Drug Enforcement Administration, Attention: CSOS Enrollment, Office of Diversion Control, E-Commerce Program (ODC), Washington, and D.C.22202. This application must be received along with or prior to any CSOS certificate applications. Registrants and POAs applying as the CSOS Coordinator will be given the option to request a CSOS certificate by indicating so on his/her application form.

(ii) Agree to all of the terms and conditions of the CP, Registrant Agreement, and the Subscriber Agreement. The agreement is presented as a "click-through" on the www.DEAecom.gov site. The Subscriber or Coordinator must accept the terms of the Agreement in order to retrieve their certificate.

3.1.2 CSOS Subscriber Registration

CSOS Subscribers must either be DEA Registrants or have been assigned POA by the Registrant to order controlled substances. To obtain a CSOS Subscriber certificate, an applicant must:

(i) Complete and submit a signed CSOS certificate application, providing all information requested by the CSOS RA without any errors, misrepresentation, or omissions.

Applications and instructions for registrants, or those who hold POA for registrants, are located on the CSOS web site, www.DEAecom.gov.

(ii) Agree to all of the terms and conditions of the CP and the Subscriber Agreement. The agreement is presented as a "click-through" on the , www.DEAecom.gov site. The Subscriber or Coordinator must accept the terms of the Agreement in order to retrieve their certificate.

(iii) Submit the application to their designated CSOS Coordinator for identity verification.

Once a Subscriber has completed the CSOS certificate application and accepted the terms and conditions of the CP and the Subscriber Agreement, the application is submitted to the CSOS Coordinator for identity and authorization verification. The CSOS Coordinator must sign the certificate application, supplying all requested information. The CSOS Coordinator must then submit all verified applications for certificates to the CSOS RA. Applications received directly from the applicant or missing the CSOS Coordinator's signature will not be processed.

Upon receipt of the application packet(s) by the CSOS RA, a CSOS RA Operator verifies the information contained in the CSOS certificate application against DEA's Controlled Substance Act (CSA) database. The PMA will ensure that CSA database information is readily available for verification.

Upon application approval, the CSOS RA notifies the CA of approval and the CA issues a CSOS certificate to the applicant. If the application is denied the CSOS RA will use reasonable efforts to notify the applicant and the applicant's CSOS Coordinator by electronic or postal mail of the refusal and reasons for the refusal.

In the event of successful adjudication of a CSOS certificate application; the applicant will receive notice of where to access the CSOS CA and how to generate the private and public keys and retrieve the CSOS certificate. The applicant's CSOS Coordinator will also receive notice that the applicant has been approved for a CSOS certificate.

3.1.3 Types of Names

Names of certificate subjects must be X.500 Distinguished Names (DN) using a set of the following X.520 naming elements: C; O; OU; and CN.

3.1.4 Need for Names to be Meaningful

All certificates issued by the CSOS CA contain the DN of C=US, O=U.S. Government, OU=Department of Justice, OU=DEA, OU=Diversion Control, OU=E-Commerce, OU=CSOS, OU="State". Subscriber certificates will include the common name (CN) of the individual using the certificate and a serial number that is unique to the Subscriber. The presence of the unique serial number guarantees that although the CN may not be unique, the DN will always be unique to each Subscriber.

The CN will be generated according to these rules:

- From the Subscriber's legal name as it appears on the DEA Form 223.
- If this name cannot be used, the name that Federal or local records refer to that person as (e.g., POA letter, human resources documents, birth certificate or drivers license) will be used.

In the event that a person is known by a name that is different then the name used to create the CN, additional CN values maybe added—at the request of the Subscriber—to the CN attribute after the DN has been formed. If these rules cannot resolve any naming issue, the issue will be resolved by the PMA according to the procedures in Section 2.4.3 of this document. The certificate subject field is the identity of the Subscriber who is being assigned the certificate from the issuing CA.

3.1.5 Rules for Interpreting Various Name Forms

DNs and their component Relative Distinguished Names (RDNs) are to be interpreted as defined in the applicable certificate profile and in Sections 3.1.3 and 3.1.4 of this CPS. The *DEA Diversion Control E-Commerce System Certificate and CRL Profile* document established by the DEA contain the rules for interpreting name forms. These documents may be found at www.deadiversion.usdoj.gov/ecomm/csos/ or , www.DEAecom.gov.

3.1.6 Uniqueness of Names

Names will be unambiguously defined for each Subscriber, as described in the preceding subsections. As stated in Section 3.1.4, the presence of the unique serial number guarantees that although the CN may not be unique, the DN will always be unique to each subscriber. Certificates issued to the CA or RA (i.e. service accounts) will have the service account name contained in the CN, however will not include the S/N. It is the responsibility of the CA to resolve all conflicts to ensure that name uniqueness is maintained.

3.1.7 Name Claim Dispute Resolution Procedure

The OMA will refer disputes with names, including disputes involving trademarked names, to the PMA for resolution. The CSOS PMA is ultimately responsible for resolution of any name claim disputes within the CSOS PKI and may direct the revocation and re-issuance of any affected certificates. The CSOS PMA will provide the CSOS RA with the results of their decisions who, in turn, will notify the applicant and CSOS Coordinator via email or postal mail.

3.1.8 Recognition, Authentication and Role of Trademarks

Certificate subject names issued under this policy will be chosen by the CA. The CA is not obligated to research trademarks or resolve trademark disputes. The CA or its agents may refuse to accept a name known to be a trademark of someone else, or deemed inappropriate for use in the certificate.

3.1.9 Method to Prove Possession of Private Key

CSOS Subscribers generate their own keys within their system as an automatic process described in Section 4.2.1. For signature public keys, the corresponding private key automatically signs the certificate request generated by the Subscriber. Verification of the signature using the public key in the request will serve as proof of possession of the private key.

The CSOS CA does not verify the uniqueness of Subscriber public keys during the certificate issuance process. Proof-of-possession of the private key is required before getting a certificate from the CA, preventing malicious attempts to re-use a public key. Client-side key generation modules are required to be FIPS-validated, which gives a high degree of confidence in the entropy of the random number generation.

3.1.10 Authentication of Organization Identity

CSOS CA certificates are issued to organizations for the purpose of cross-certification only and require PMA approval in advance of issuance. The RA will verify organizational identity using third-party knowledge broker data, D&B listings, etc. and will provide the results of this information and the tools used for verification at the time the request is provided to the PMA for review.

3.1.11 Authentication of Individual Identity

3.1.11.1 CSOS Coordinator Identification Process

A Principal Coordinator and optional Alternate Coordinator will be identified for each DEA Registrant (as indicated on DEA Form 223) participating in the Controlled Substance Ordering System. The Principal Coordinator will serve as an organization's primary recognized CSOS contact for the DEA Registrant(s) identified on their application. The Principal Coordinator applicant may be any individual employed or contracted by the organization designated to serve in that role. If a CSOS DEA Registrant Certificate Application is submitted, the DEA Registrant will serve the role of Principal Coordinator unless otherwise indicated on the application.

A CSOS Coordinator application must be received by the CSOS RA along with, or prior to, any CSOS Subscriber certificate applications. CSOS Coordinators will submit the following information/credentials to the CSOS RA for identity verification:

- A signed and notarized CSOS Coordinator application obtained from the CSOS Web site. This application must be signed by the same individual who has signed the most recent application for DEA Registration (DEA Form 223) and authorizes that individual listed on application to represent the organization in the capacity of the CSOS Coordinator.

- Two copies of identification, one of which must be a government-issued photo ID, such as a driver's license or passport.

- A copy of a current DEA Registration (Form 223) or the most recent application for DEA registration in the event that application for DEA Registration and a CSOS Coordinator certificate are simultaneously submitted.

- For individuals granted Power of Attorney (POA) to sign orders for controlled substances on behalf of a DEA Registrant, a copy of the POA assignment letter as specified in Title 21 Code of Federal Regulations (CFR).

The CSOS RA notifies the applicant via e-mail upon receiving the application package and adjudicates the applicant through the following procedures:

- Validates that all required information and documentation has been provided.

- Validates that the Notary information is complete, identification documents match information provided on the application, and through performing an out-of-band telephone verification of employment, position, and location through organization's Human Resource department or with the owner/operator of smaller business entities.

- Validates the DEA Registrant(s) provided information, including business activity, schedules and DEA Registration expiration date against DEA CSA data provided by DEA.

- Verifies the organization mailing address and the employment of the individual at the provided address.

3.1.11.2 CSOS Subscriber Identification Process

Authentication of Subscriber identity is performed by the local organization and requires the delegation of a CSOS Coordinator, who serves as the Local Registration Authority (LRA) and organizational point of contact for CSOS issues. Subscribers will submit the following information/credentials to their designated CSOS Coordinator for identity verification:

- A CSOS Certificate application, signed by the applicant, stating that the applicant has read and understands the terms of the DEA Diversion Control E-Commerce System Certificate Policy and has agreed to the statement of Subscriber obligations in the Subscriber Agreement;

- Two copies of identification, one of which must be a government-issued photo ID, such as a driver's license or passport;

- For individuals with power of attorney (POA) to sign orders for controlled substances, a copy of the POA assignment letter as specified in Code of Federal Regulations (CFR).

- A notarized CSOS Certificate Application Registrant List Addendum used for individuals who wish to apply for a CSOS Certificate for more than one DEA

Registrant. Up to 5 Addendums may be submitted to specify up to 51 different DEA Registrants. (Practice note: this event occurs when a single individual is granted multiple POA to order for several DEA Registrants (registered locations). An example is with chain pharmacies where a single individual orders controlled substances for all company locations).

The Principal Coordinator/Alternate Coordinator adjudicates the Power of Attorney applicant. This includes validating the following:

- All required information/documentation is provided.
- Applicant identity is adjudicated as specified in the DEA Registrant agreement.
- The Affirmation of Identity Verification section of the application is signed by the Coordinator.

The Coordinator maintains a copy of the application package and the method by which the identity was verified for their records. Upon signing the application, the Coordinator forwards, via postal mail, the application packet to the CSOS RA.

The CSOS RA notifies the applicant and Principal Coordinator/Alternate Coordinator via e-mail upon receiving the application package. The CSOS RA then validates that the application has been properly completed with all required information and documentation provided. The RA then cross-references application information with relevant information from the CSA database.

The required steps the RA Operator must complete for each application type are summarized in Table 3–1, Adjudication Procedures:

Adjudication Procedures			
	Application Type		
Steps	**Registrant**	**Coordinator**	**POA**
1. All of the application fields are complete and valid	✓	✓	✓
2. All required signatures are present.	✓	✓	✓
3. Identification documents provided match the individual represented on the application.	✓	✓	✓
4. The signature on the application is similar to the signature on the identification documents provided.	✓	✓	✓
5. Applicant is presently employed by the organization identified on the application.	✓	✓	
6. Applicant's place of employ matches business address presented on the application.	✓	✓	
7. The address of the organization must match the organization address provided on the		✓	

Adjudication Procedures			
	Application Type		
Steps	Registrant	Coordinator	POA
application.			
8. Power of Attorney documentation is present for the DEA Registration(s) identified on the application		✓*	✓
9. Proof of DEA Registration (Form 223 or the application for DEA Registration)	✓	✓	
* POA form is only necessary if Coordinator is applying for a POA certificate.			

Table 3–1. Adjudication Procedures

3.1.11.3 CSOS Subscriber Bulk Enrollment

DEA issues a separate DEA Registration to each location authorized to handle controlled substances. In some business cases, such as with chain pharmacies utilizing a centralized ordering business model, a single individual may be assigned the responsibility for ordering controlled substances for many different locations, some with different authorized controlled substance schedules. Thusly, under CSOS, a single individual would need to hold separate digital certificates for each registered location – using that Registrant's certificate to sign orders for controlled substances authorized for delivery to that location. To accommodate these business cases within CSOS, DEA has established Bulk Enrollment procedures.

In order to participate in CSOS Bulk Enrollment, an organization must currently participate in the DEA Chain Renewal program. The Chain Renewal procedure, described at http://www.deadiversion.usdoj.gov/drugreg/chain_renewal.htm, was developed by DEA to simplify the renewal application process for companies that maintain registrations at multiple locations, for example chain pharmacies. The procedure allows corporations to renew all of their DEA registrations at the same time, thereby eliminating the need for multiple applications. This simplified application process is available to corporations with 50 or more retail pharmacy registrations or distributors with 10 or more registered locations.

To enroll in CSOS under Bulk Enrollment processes, each applicant (DEA Registrant, Principal Coordinator, Alternate Coordinator, and POA), will complete his/her application as specified in the above processes with the exception of how the DEA Registration and POA documentation is submitted. The CSOS RA will work with the organization's primary point of contact for bulk enrollment to ensure the DEA Registration and POA documentation are submitted correctly.

For the DEA Registrations for which the applicant is applying, the organization will provide the following:

- A printed list of the DEA Registrations (including all pertinent information such as DEA Registration Number, name, address and current expiration date) listed in order by DEA Registration Number.

- A 3.5" diskette or CD with the DEA Registration Numbers only in alphanumeric order in ASCII format.

- For POA applicants, the organization will provide a single POA listing all of the DEA Registration Numbers for which the applicant is applying.

3.1.11.4 Authentication of Component Identities

The CSOS CA will issue administrative digital certificates to:

Text removed. Information representing “critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities” has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.

These certificates differ from CSOS Subscriber certificates in that they do not assert the OID of the DEA Diversion Control E-Commerce System OID and are not populated with DEA extension data. DEA Regulations (specified in the 21 U.S. Code of Federal Regulations) prohibit the use of digital certificates not containing this extension data for controlled substance ordering.

Administrative certificates issued by the CSOS CA must be associated with a PKI sponsor. Requests for certificates are submitted to the CSOS RA by the Operations Manager and include the following information:

- Date of Request

- Employee Name

- Employee ID#

- Certificate Distinguished Name (DN) as the unique identifier for the certificate

- Reason for request

- Transfer of ownership (if applicable)

- If the request is for a component, the request must include the equipment identification information (serial number) or service name (DNS name)

- Contact information to enable the CA or CSOS RA to communicate with the PKI sponsor

- The Operations Manager's signature to indicate request approval.

The CSOS RA will confirm the identity of the applicant through visually inspecting the employee's badge information and photo, and validate that the badge contains a green diamond that indicates that the employee has the required DEA security clearance. Upon successful adjudication, the CSOS RA will sign the request form.

The applicant then provides the signed request form to the CSOS CA, who will generate a certificate request and ensure that the sponsor retrieves the certificate in a manner that guarantees that the private key remains under the sole control of the employee.

Upon retrieval of the certificate, the request form is updated to include the certificate DN as discussed above and the signed request is provided to the Security Officer to file.

Administrative, device and component certificates are issued for a period not to exceed three years. Upon expiration or update, the user associated with the device or component certificate must complete a new request for a certificate, using the procedure outlined above.

Administrative, device and component certificates are revoked immediately upon the sponsor or individual's employment termination with CSOS or upon notification to the RA of suspected compromise.

The Operations Manager completes and signs revocation requests, indicating the date and reason for the request on the original form obtained from the Security Officer and then distributing the form to the CA Operator for action and signature. This form is then provided to the Security Officer to be archived.

3.2 Routine Re-key

3.2.1 CSOS Subscribers

The Subscriber, through the CSOS Coordinator, may request that the CA issue a new CSOS certificate containing a new serial number with a new key pair, provided that the original certificate has not been revoked and the Subscriber is in good standing with the CA, continuing to qualify as a DEA registrant or POA, as defined in Section 1.3.7. The DEA Diversion Control E-Commerce System CP does not permit Subscriber certificate renewal (issuance of a new certificate for an existing key pair).

Re-key requests can be authenticated on the basis of the CSOS Coordinator's digital signature using the current private key for a total of two certificate requests beyond the initial request. Upon the third certificate request, Subscribers will be required to establish identity using the initial registration process described in Sections 3.1.11.2 and 4.

The CSOS RA will send an automatically scheduled email notifying the Subscriber and the Subscriber's CSOS Coordinator 45 days prior to the expiration date of the Subscriber's CSOS certificate. The CSOS Coordinator will receive two notifications at this time, the first notification contains a listing of Subscribers who have renewed twice previously and are now required to renew via the initial enrollment process, and the second notification contains a listing of CSOS Subscribers who are eligible for electronic renewal. After confirming that the information in the listing is accurate, the CSOS Coordinator will return a digitally signed reply to the CSOS RA, using their CSOS issued certificate, to request that new Subscriber certificates be issued to these Subscribers.

All re-key requests are adjudicated by the CSOS RA and checked to ensure 1) that the digital signature signing the request is validated against the one issued to the Subscriber or Coordinator, 2) checked to ensure that the certificate has not been revoked or suspended, and 3) checked against the CSA database to ensure that the extension data is still valid. After adjudication, the request is entered into the RA database and sent to the CSOS CA as previously discussed.

DEA updates its CSA database upon the receipt of information changes from the Registrant and from Registration renewal requests from the organization with whom the CSOS Coordinator is associated.

In the event that there is a discrepancy between the data in the CSA database and the Subscriber's data, and provided that the request for a new CSOS certificate has been submitted prior to the DEA's Registration and Subscriber certificate expiration and that it is not the third renewal request:

- The renewing Subscriber's request will be placed into an update queue for processing until the CSA database is appropriately updated with the Subscriber's new DEA Registration information. This request will be held for a maximum period of 90 days to allow the information to be updated in the CSA database. This, then, does not require the resubmission of a complete application even in the event that the existing Subscriber certificate expires during this period.

- Subscribers and Coordinators receive an email notification that there is a Registration information discrepancy that needs to be resolved with DEA. A second notification is sent from the CSOS RA at 45 days.

- When the CSA database update agrees with the applicant data, and the CSA extract is received by the CSOS RA, the application is automatically removed from its hold status and a notice sent to the Subscriber and CSOS Coordinator with instructions on how to retrieve their new certificate.

Under normal circumstances, Subscribers and Coordinators not receiving their certificates within 10 business days from the receipt of CSOS RA notification of the submission package can contact the CSOS Help Desk to check status.

Requests for new certificates due to name changes (e.g. due to marriage) require proof of the name change be provided to the CSOS Coordinator, or other designated agent. The CSOS Coordinator will serve as the certifier for the name change request submitted to the CSOS RA. Requests for new certificates due to a change of other information present in the Certificate extension data (reduction or addition of controlled substance ordering authorization, Registrant address or DEA Registration number) requires the Subscriber to establish identity using the initial registration process described in Sections 3.1.11.2 and 4.

3.2.2 CSOS CA Re-Key

The DEA Diversion Control E-Commerce Bridge CA is a self-signed root. Both the DEA Bridge CA and the CSOS Subordinate CA generate and store their private keys using a FIPS 140 level three certified Hardware Security Module (HSM). Re-keying of the DEA Bridge CA is completely internal to the CA and the generation of the CA's new keys takes place within the HSM. The DEA Bridge CA key pair and certificate will not exceed the lifetimes stated in the CP. The Root and CSOS CA Key Changeover Schedule are provided in system documentation.

The CSOS CA will participate in an offline subordination process with the DEA Bridge CA at the time of re-key. The subordination process (in which the DEA Bridge CA signs the CSOS CA's certificate) will be done using removable media transferred between the two CAs. The entire process is contained within the domain of the two CAs. No outside entities are involved in the subordination process. As with the DEA Bridge CA, the CSOS CA's certificate and public and private key lifetimes will not exceed the durations set forth in the Diversion CP.

The new public key will be posted on the Web site at www.DEAecom.gov and notification of the re-key will be provided through a digitally signed email from the CSOS RA to the CSOS Coordinators.

3.3 Re-key After Revocation

In the event of certificate revocation for reason of key compromise, cessation of operation, or as a result of negative action taken against the Registrant or Subscriber by DEA, issuance of a new certificate always requires that the Subscriber go through the initial registration process as described in Sections 3.1.11.2 and 4. Certificate revocation due to a technical malfunction that makes the private key invalid will not require renewal via initial enrollment provided that the previous adjudication was performed within 60 days of certificate revocation and the renewal request has been approved by the CSOS Coordinator.

3.4 Revocation Request

Requests for certificate revocation will require either verbal authentication using a security code known only to the Subscriber and the RA, or a signature on the revocation request from a person identified in Section 4.4.2 along with any information covered in Section 4.4 of this CPS. Electronic revocation requests will be authenticated using the certificate's associated private key, regardless of whether or not the private key has been compromised. The RA will use reasonable efforts to notify the Subscriber, Registrant, or applicable CSOS Coordinator about the revocation

of the CSOS certificate via electronic means, mail, or telephone call. Revocation request procedures are described in Section 4.4.3.

Section 4 – Operational Requirements

4.1 Certificate Application

Eligible Subscribers are those who hold a valid DEA registration as defined in Title 21 CFR Part 1300. All Subscriber applicants will submit a completed application and documents substantiating identification in accordance with Section 3.1.11.2 above, entering into an initial agreement with the CA evidenced by accepting the applicable DEA Registrant or Subscriber Agreement at the CSOS web site, prior to certificate issuance. Complete application processing information is contained in internal system documentation. Certificate application forms and instructions may be obtained from , www.DEAecom.gov. The applicant will follow the procedures in the Subscriber Manual posted on the CSOS web site at, www.DEAecom.gov, mailing completed applications to the CSOS Registration Authority at Drug Enforcement Administration, Attention: CSOS Enrollment, Office of Diversion Control, E-Commerce Program (ODC), Washington, D.C.22202.

Using the information provided with the application, the CSOS Coordinator will perform identity verification according to the requirements specified in the CP and this CPS. Subscriber applications are scanned by the RA and are entered into the RA database prior to adjudication. Based on subsequent verification against the CSA database, the CSOS RA either approves or denies the application. The CSOS RA will notify the Registrant or the Registrant's CSOS Coordinator when the application is received via digitally signed email. The CSOS RA notes all action taken on the certificate request in the CSOS RA database and retains the certificate request. Should the application be denied, the CSOS RA will provide notification of the application denial to the applicant and the applicant's CSOS Coordinator.

The procedures developed and published on the CSOS web site are included in the CSOS Subscriber Manual and are as follows:

1. The Subscriber applicant accepts the DEA Bridge CA and CSOS CA certificates from a link provided on the CSOS web site in order to trust certificates issued by the CSOS CA.

2. The Subscriber applicant downloads the applicable CSOS enrollment application. Application forms and instructions are provided for the following CSOS Subscribers:

CSOS DEA Registrant Certificate Application –The following steps outline the DEA Registrant Certificate application process:

1. The applicant reads/agrees to the DEA Registrant Agreement, the CSOS Subscriber Agreement and the CSOS Privacy Policy.

2. The DEA Registrant completes the New CSOS DEA Registrant Certificate Application and the CSOS Certificate Application Registration List Addendum(s) if applicable.

3. On the application, the DEA Registrant must designate a Principal Coordinator. The Principal Coordinator must be approved prior to the Registration Authority processing CSOS Power of Attorney or Alternate Coordinator certificate applications. These Coordinators serve as the organization's Local Registration Authority (LRA).

4. The DEA Registrant has the application and addendum(s) (if applicable) notarized.

5. The DEA Registrant attaches a photocopy(ies) of the DEA Registration Certificate(s) for the DEA Registration(s) identified, and photocopies of their identification documents and then mails the application package to the CSOS Registration Authority.

6. The CSOS Registration Authority notifies the DEA Registrant via e-mail upon receiving the application package.

7. The Registration Authority verifies the identity of the DEA Registrant and validates the DEA Registration(s) identified.

8. Upon approval, the CSOS CA sends the authorization and reference code(s) to the DEA Registrant. The reference code(s) is sent via e-mail. The authorization code(s) is sent via postal mail to the address provided by the CSOS Coordinator on the application in a tamper evident envelope.

9. After receiving the authorization and reference code(s), the DEA Registrant returns to the CSOS Web site to retrieve his/her CSOS Certificate(s).

CSOS Principal Coordinator/Alternate Coordinator–A Principal Coordinator must be approved prior to the Registration Authority processing CSOS Power of Attorney or Alternate Coordinator certificate applications. The following steps outline the CSOS Principal Coordinator / Alternate Coordinator application process:

1. The DEA Registrant designates the CSOS Principal Coordinator/Alternate Coordinator applicant for the DEA Registration(s) identified.

2. The applicant reads/agrees to the DEA Registrant Agreement, the CSOS Subscriber Agreement and the CSOS Privacy Policy.

3. The applicant completes the application and has the application signed by the DEA Registrant.

4. The applicant has the application and addendum(s) (if applicable) notarized.

5. The applicant attaches a photocopy(ies) of the DEA Registration Certificate(s) and Power(s) of Attorney (if applicable) for the DEA Registration(s) identified and photocopies of their identification documents, and then mails the application package to the Registration Authority.

6. Once the Registration Authority receives the application package, the Registration Authority notifies the applicant via e-mail upon receiving the application package.

7. The Registration Authority verifies the identity and applicability of the applicant and validates the DEA Registration(s) identified.

8. Upon approval, the CSOS CA sends the authorization and reference code(s) to the applicant. The reference code(s) is sent via e-mail. The authorization code(s) is sent via postal mail to the address provided on the application.

9. After receiving the authorization and reference code(s), the applicant returns to the CSOS Web site to retrieve his/her CSOS Certificate(s).

CSOS Power of Attorney Certificate Application–A Principal Coordinator must be approved prior to the Registration Authority processing CSOS Power of Attorney or Alternate Coordinator certificate applications. The following steps outline the CSOS Power of Attorney Certificate application process:

1. The applicant reads and agrees to the CSOS Subscriber Agreement and the CSOS Privacy Policy.

2. The applicant completes the CSOS Power of Attorney Certificate Application.

3. The applicant attaches the CSOS Certificate Registration List Addendum(s) (if applicable) and the Power(s) of Attorney for the DEA Registration(s) identified and then forwards the application to either the Principal Coordinator or the Alternate Coordinator.

4. The Principal Coordinator/Alternate Coordinator adjudicates the Power of Attorney applicant as defined in the DEA Registrant Agreement.

5. The Principal Coordinator/Alternate Coordinator forwards the original application package to the Registration Authority.

6. Once the Registration Authority receives the application package, the Registration Authority notifies the applicant and Principal Coordinator/Alternate Coordinator via e-mail upon receiving the application package.

7. The Registration Authority validates the application and DEA Registration(s) identified.

8. Upon approval, the Registration Authority sends the reference code(s) to the applicant via e-mail. The authorization code(s) is sent by the Principal Coordinator/Alternate Coordinator via postal mail. The Principal Coordinator/Alternate Coordinator must forward the sealed authorization code(s) to the applicant.

9. After receiving the authorization and reference code(s), the applicant returns to the CSOS Web site to retrieve his/her CSOS Certificate(s).

Bulk Enrollment Applications–In order to participate in CSOS Bulk Enrollment, the applicant must be applying for more than 50 CSOS Certificates and the organization must currently participate in the DEA Chain Renewal program for DEA Registrations. Bulk Enrollment has been established to accommodate organizations that need to obtain a large volume of CSOS Certificates associated with a single applicant. Each applicant, DEA Registrant, Principal Coordinator, Alternate Coordinator, and Power of Attorney, will complete his/her application as previously specified with the exception of how DEA Registration and Power of Attorney documentation is submitted. DEA Registration and Power of Attorney documentation will be submitted as described below. The CSOS Registration Authority will work with the organization's primary point of contact for bulk enrollment to ensure the DEA Registration and Power of Attorney documentation is submitted correctly.

1. For the DEA Registrations for which the applicant is applying, the organization will provide the following:

- A printed list of the DEA Registrations (including all pertinent information such as DEA Registration Number, name, address and current expiration date) listed in order by DEA Registration Number.

- A 3.5" diskette or CD with the DEA Registration Numbers in alphanumeric order only, saved as an ASCII text file.

This information is mailed to: Drug Enforcement Administration, Office of Diversion Control, E-Commerce Program (ODC), Attention: CSOS Bulk Enrollment, Washington, D.C.22202.

2. For Power of Attorney applicants, the organization will provide a single Power of Attorney listing all of the DEA Registration Numbers for which the applicant is applying.

3. The Organization provides a contact point including Corporate Name, address, telephone number, fax number, individual contact and alternate contact for the bulk enrollment process.

4. Upon receipt of the package, the CSOS Registration Authority validates the application and DEA Registration(s) identified.

5. Upon approval, the CSOS CA creates two ASCII files, one containing the reference codes and one containing the authorization codes for the DEA Registrants identified. The reference code file is sent to the applicant via e-mail. The authorization code file is sent on compact disk (CD) to the address provided by the Coordinator via postal mail. The Principal Coordinator/Alternate Coordinator must forward the sealed authorization code(s) to the applicant.

6. After receiving the authorization and reference code(s), the applicant returns to the CSOS Web site to retrieve his/her CSOS certificate(s).

4.2 Certificate Issuance

4.2.1 Subscriber Certificate Issuance

The following represents a sanitized statement of the Subscriber certificate issuance process. Information representing "critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities" has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.

Subscriber information is verified against a daily extract of DEA Registrant information contained in DEA's CSA database.

The CSOS RA validates subscriber information for completeness and accuracy and enters the data into the CSOS CA system. Errors detected at this point will be reported to the CSOS RA, who, in turn, notifies the applicant and their CSOS Coordinator via email. It is the CSOS Coordinator's responsibility to contact DEA to resolve errors in the CSA database.

The unique identification number of the identifications presented is recorded on the DEA Registrant and Coordinator Applications by the Notary Public and the photocopy of the identification documents are filed with the application and are also contained with the image of the application created during document scanning. Applications and photocopies of identification documents are stored in locked file cabinets with access limited to authorized individuals with a need-to-know.

CSOS software automatically processes the certificate request, populating the certificate extension data from the DEA CSA database information, signs the signing public key certificate, and stores a copy of the certificate in the CSOS CA database.

Upon successful adjudication, the CSOS RA submits applicant information to the CSOS CA, instructing the CA to issue the certificate to the applicant. The CA provides the individual with one-time use reference and authorization codes in two separate out-of-band processes.

The CSOS CA then provides a copy of the signing public key certificate to the client electronically through the program during the session. Next, the CSOS CA writes the public certificate into the CSOS repository. The issuance of a certificate by the CSOS CA indicates the end of the certificate issuance process. Subscriber acceptance of the certificate is covered in the following section.

For bulk enrollments, The CSOS RA adjudicates the applicant as previously discussed, and associates the applicant with the Principal Coordinator for the DEA Registrations identified in the Registration Authority database. Upon approval, the CSOS CA creates two ASCII files, one containing the reference codes and one containing the authorization codes for the DEA Registrations identified. These files are sent in separate out-of-band processes to the designated responsible party at the applicants' organization. Instructions are provided to the Subscriber for accessing the secured CSOS Web site and retrieving the certificates.

The CSOS CA software automatically verifies the certificate request, signs the signing public key certificate, and stores a copy of the certificate in the CSOS CA database. The CSOS CA then provides a copy of the signing public key certificate to the client electronically through the program during the session. Next, the CSOS CA writes the public certificate into the CSOS repository. The issuance of a certificate by the CSOS CA indicates the end of the certificate issuance process. Subscriber acceptance of the certificate is covered in the following section.

The CSOS CA software automatically validates certificate information prior processing a certificate request. Validation is performed on the controlled substance schedules that the Subscriber can order, business activity and DEA Registrant location contained within the customized certificate extension to ensure that the data is accurately populated in the Subscriber certificates.

The RA workflow and certificate issuance processes are monitored to ensure that these processes continue to compare favorably with baseline performance metrics.

4.2.2 CSOS CA Certificate Issuance

The CSOS CA receives its initial subordination certificate signed by the DEA E-Commerce Bridge during a Key Generation ceremony audited by KPMG. Following is a summary of the procedures followed during this process:

1. The CSOS CA generates a signed certificate request (PKCS #10) that is saved to removable media.

2. The certificate request is delivered to the DEA Bridge CA, which serves as the CSOS CA's root CA.

3. The DEA Bridge CA signs and returns a PKCS7 response to the CSOS CA, saved on removable media.

4. The CSOS CSA will post the signed certificate in the CSOS Repository.

4.3 Certificate Acceptance

Acceptance of the certificate occurs when the Subscriber uses the auth/ref codes distributed by the RA and their CSOS Coordinator to generate a certificate request and retrieve the certificate. The operation of the secure communications protocol between the Subscriber and the CSOS CA involves the mutual authentication of the two parties along with both the request and the response operations that constitute acceptance by the Subscriber of the resulting public key certificates. This process is also covered in Section 6.1.3 of this document.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for Revocation

4.4.1.1 Subscriber Certificates

The CSOS RA electronically receives a daily CSA database extract file from DEA through a secured connection to

Text removed. Information representing “critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities” has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.

A certificate will be revoked in accordance with Section 4.4.9.1 when the binding between the Subscriber and the Subscriber’s public key defined within the certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

- Change of identifying information or affiliation components of any names in the certificate (i.e. Subscriber name change);
- Privilege attributes asserted in the Subscriber's certificate are reduced (i.e. controlled substance ordering schedules reduced);
- Compromise or suspected compromise of private keys, private key storage media and/or user password;
- Forgotten password or the Subscriber’s private key cannot be accessed for any reason;
- The Subscriber, the DEA Registrant under whose Registration a certificate holder obtained a certificate, or CSOS Coordinator requests that the affiliated Subscriber certificate be revoked;
- It can be demonstrated that the Subscriber has violated the stipulations of the Subscriber Agreement;

- Corporate mergers or takeover;
- DEA posts notice that certificate holder's DEA Registration has been revoked, suspended or restricted, that the Registration information has changed, or that the Registration has been terminated;
- Cessation of CA operations or suspected key compromise of the CSOS CA or the DEA Bridge CA following PMA approval.

Due to the negative financial impact on the CSOS community, the CSOS CA certificate and the CSOS Subscriber certificates will not be immediately revoked as a result of negative audit findings provided by the third-party auditor against the CSOS CA, unless findings indicating key compromise have been substantiated and the PMA majority vote deems it necessary to implement the key compromise plan. Suspension of new certificates until audit discrepancies are resolved, however, may be directed by the PMA.

Upon revocation of the Subscriber's certificate, the Subscriber and the CSOS Coordinator are notified via e-mail.

4.4.1.2 CSOS CA Certificate

The CSOS CA certificate can be revoked under the following circumstances:

- When the PMA requests that the certificate be revoked in the event that the PMA determines that the CSOS CA does not meet policy requirements or that the system is no longer in the best interest of the federal government.
- When the DEA Diversion Control E-Commerce System PMA determines that an emergency has occurred that may impact the integrity of the certificates issued by the DEA Diversion Control E-Commerce System.
- In the event of suspected key compromise of the DEA Bridge CA or CSOS CA.

In the event of key compromise or under direction of the PMA, the CSOS CA has the ability to support the secure and authenticated revocation of one or more certificates of one or more Subscribers and provides a means of rapid communication of such revocation through the issuance of daily CRLs (or, if necessary, more frequent CRLs). The CA's system and processes provide the capability to revoke the set of all certificates issued by the CSOS CA that have been signed with the CSOS CA's private signing key. A script that can immediately send a signed email to all CSOS Coordinators has been developed and is maintained under the dual control of the RA Manager and Ops Manager. The procedures for its execution are maintained in internal system documentation.

The DEA Diversion Control E-Commerce System has a key compromise plan that details the circumstances and procedures to be implemented by the PMA and OMA when CA key compromise is suspected, or other incident occurs that may adversely impact the integrity of the certificates issued by the CA.

Revoked certificates will continue to be included on all new publications of the certificate status information for a period in excess of 60 days beyond certificate expiration. CSOS Relying Parties are permitted under 21CFR 1305.09 to fill received orders for 60 days after the execution

of the order by the purchaser, provided the order was valid at the time of signing. Continuing to maintain revocation information on the CRL until 60 days beyond expiration ensures that a revoked certificate is not validated during this period. Complete revocation processing information is contained in the *Revocation Process* document.

The CSOS CA is not responsible for Subscriber token (hardware or software) maintenance or destruction when a Subscriber ceases its relationship with an organization that sponsored the certificate. Subscribers and organizations have been directed through the Certificate Policy and Federal Regulations to require the Subscriber to surrender to that organization (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of the sponsoring organization. They must then zeroize or otherwise destroy promptly upon surrender, protecting the token from malicious use between surrender and zeroization or destruction. If a Subscriber leaves an organization and the hardware tokens cannot be obtained from the Subscriber, then the CSOS Coordinator must immediately request that all Subscriber certificates associated with the unretrieved tokens be immediately revoked.

4.4.2 Who Can Request Revocation

The revocation of a certificate may only be requested by:

- Subscriber
- Subscriber's Sponsoring Organization
- Subscriber's CSOS Coordinator
- DEA PMA

If an organization's DEA Registration information has changed or the DEA Registration is revoked, every certificate issued for that DEA Registration will be revoked. This request is generated from either the Controlled Substance Act (CSA) database or the organization via authenticated telephone request or digitally signed email request. If the request is generated by the organization, only the DEA Registrant or the CSOS Coordinator may submit the requests. The Subscriber (individual), the CSOS Coordinator, or the DEA Registrant may request revocation of all certificates issued to an individual.

4.4.3 Procedure for Revocation Request

The following represents a sanitized description of revocation request procedures. Information representing "critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities" has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.

Subscriber certificate revocation procedures are detailed in internal system documentation and are summarized in this section. Revocation requests can be made by digitally signed email to **csosrevocation@DEAecom.gov.** Revocation requests due to key compromise may be submitted by telephone to 1-800-DEA-ECOM (332-3266). Revocation requests must be authenticated as follows:

All revocation requests will include the following information:

- Subscriber's full name;
- Subscriber's work e-mail address (if applicable);
- Date of revocation request;
- Reason for revocation;
- Date of compromise;
- Digital signature of one of the parties identified in Section 4.4.2.

Certificate(s) revocation requests are given priority attention over other certificate actions. Authenticated revocation requests are entered into the RA database and a request is sent to the RA such that updated certificate status will appear on a CRL within 6 hours of receipt of the compromised revocation request.

Upon authentication, the RA will authorize the CA to execute the revocation request. In the event of suspected compromise, the Subscriber, or other authorized person, can request revocation via a telephone call to the RA. All revocation requests are authenticated and revocation requests and actions are retained, including a date stamp on the action.

Revocation reason codes have been developed specifically to meet DEA's business cases. The revocation reason is conveyed by the use of an optional revocation flag that is associated with every certificate placed on the CRL. The following table maps DEA's certificate revocation codes to specific business cases and reasons necessitating revocation:

Reasons for Revocation		
Revocation Reason	**Generated By**	**Certificate Reason Code**
Key Compromise	Subscriber	Key Compromise
Subscriber Name Change	Coordinator or Registrant	Affiliation Change
Subscriber E-mail Address Change	Subscriber	Affiliation Change
DEA Registrant Name Change	CSA	Affiliation Change
DEA Registrant Address Change	CSA, Coordinator or	Affiliation Change

Reasons for Revocation		
Revocation Reason	**Generated By**	**Certificate Reason Code**
	Registrant	
Schedule Addition / Reduction	CSA	Affiliation Change
Change of Business Activity	CSA	Affiliation Change
Registration Surrendered for Cause	CSA	Cessation of Operation
Registration Revoked	CSA	Cessation of Operation
Registration Out of Business	CSA	Cessation of Operation
Registration Suspended	CSA	Certificate Hold
Registration Restricted for Cause/CA Administrative Action	CSA	Superseded
Lost/Forgotten Password	Subscriber	Superseded
Order to show cause	CSA	Certificate Hold

Exhibit 4–1. Revocation Reason Codes

4.4.4 Revocation Request Grace Period

When a key compromise is detected, suspected, or when discovered risk is determined to warrant revocation, all certificate holders/subscribers are required to immediately notify CSOS RA so that the certificate can be revoked.

4.4.5 Circumstances for Suspension

At their discretion, the PMA may choose to request Subscriber certificate suspension, rather than revoke the Subscriber certificate. Examples of circumstances under which the PMA may choose suspension include:

- As a result of a discrepancy reported in compliance audit of a subordinate or cross-certified CA, the PMA may choose to suspend rather than revoke the CA's certificate until the discrepancy has been corrected.

- Subscriber certificates may be suspended if the status of the Subscriber has changed and the PMA deems it appropriate to suspend rather than revoke the Subscriber certificate.

- Under certain circumstances, such as when an investigation is proceeding against a Subscriber or Registrant, DEA may choose to suspend, rather than revoke, one or more digital certificates associated with the investigation.

4.4.6 Who Can Request Suspension

Only the PMA has been assigned the authority to issue a suspension request. Suspension requests received from Subscribers, Registrants or Coordinators are not valid and will not be processed. Suspension-related requests received from the PMA are authenticated through a callback to a phone number of record for the identity making the request or by a digitally signed email request.

4.4.7 Procedure for Suspension Request

Suspension requests received from the PMA are processed as follows:

1. The PMA member requesting suspension will provide the CSOS Help Desk with a written request for certificate suspension. This letter or email will specify whether the suspension will be for a specific Subscriber, all certificates issued for one or more DEA Registrants, all Subscribers coordinated by one or more CSOS Coordinators, all certificates issued by a CA based on a single public/private key pair used by a CA to generate the certificates, or all certificates issued by a CA, regardless of the public/private key pair used.

2. All suspension requests must be authenticated prior to any certificate action being performed. Authentication is performed by verbal acknowledgement from the DEA E-Commerce Section Chief or his vice that the request is valid. The Help Desk staff member handling the suspension request will annotate on the suspension request the date and time the confirmation was received and will initial the letter. A copy of this letter will be provided to the SO to be taken to the archive facility.

3. In the event that the PMA requests suspension of all certificates issued by the CSOS CA, or suspension of certificates issued by a specific CSOS CA key pair, the suspension request will be authenticated by both the DEA E-Commerce Section Chief and the Operations Manager, with the date and time authentication was received recorded and initialed by both the DEA E-Commerce Section Chief and the Operations Manager on the written request. A copy of this letter will be provided to the SO to be taken to the archive facility.

4. Suspension requests from the PMA are handled with the same priority attention as revocation requests and are addressed prior to other certificate requests.

5. Notice of the certificate suspension is provided to the Subscriber’s Coordinator or Registrant immediately via email from the CSOS RA.

6. The CSOS RA inserts the suspension request into the electronic revocation workflow and sent to the CSOS CA.

7. The CSOS CA will process the suspension request by setting the CRLReason code as ‘certificateHold’ on the CRL for the duration of time in which the certificate is suspended or expires.

8. The suspended certificate will remain on the CSOS CA’s CRL with its original actin date and expiration date until the CSOS RA is notified via telephone, email, or written notice from a DEA E-Commerce Section Investigator that the certificate should no longer be suspended, or for a period exceeding 60 days beyond the certificate expiration date. Request for removal of the suspension must be provided in writing from the DEA E-Commerce Section Chief or Operations Manager.

9. The CSOS RA will process the suspension removal request by inserting the removal request into the electronic workflow system.

10. The CSOS CA will remove the certificate from the CRL.

11. The CSOS RA will notify the Subscriber or Subscriber’s CSOS Coordinator via email that the certificate has been removed from suspension.

In the event that a suspended certificate transitions to a revocation status, the PMA or E-Commerce Chief will provide notice to the RA requesting a certificate revocation and will be authenticated as discussed in Step 1, above. Revocation of suspended certificates will be processed as discussed in Section 4.4.3, changing the CRLReason code to the appropriate revocation code as previously discussed. The CSOS RA will notify the Subscriber or Subscriber’s CSOS Coordinator via email that the suspended certificate has been revoked.

4.4.8 Limits on Suspension Period

Certificates will remain in a suspended status until the PMA concludes their investigation and warrants either revocation or removal from the CRL, as discussed above. Suspended certificates that expire will remain on the CRL for a period of at least 60 days beyond certificate expiration.

4.4.9 Certificate Revocation Lists (CRLs)

The CSOS CA issues Certificate Revocation Lists (CRLs) in accordance with the CRL profile provided in the *DEA Diversion Control E-Commerce System Certificate and CRL Profile* document provided on the DEA and CSOS web sites. The contents of the CRLs are checked prior to posting to the CSOS Repository to ensure information accuracy using mechanisms provided by the CA software. Repository performance is managed using automated reporting tools that alert a System Administrator in the event that the repository fails. Repository performance metrics are monitored to ensure reliability.

4.4.9.1 CRL Issuance Frequency

The CSOS CA will issue CRLs within a period not to exceed 24-hours/7 days a week, even if there are no changes to be made**.** Changes to certificate status information will be posted as follows:

Revocation Reason	**CRL will be issued:**
Revocation due to suspected key compromise, loss of Subscriber's private key storage media, lost or forgotten password.	6 hours after receiving an authenticated revocation request.
Revocation for reasons other than key compromise or loss.	At least once each day.

Exhibit 4–2. CRL Issuance Frequency

New CSOS CRLs are immediately published in the CSOS CA repository, overwriting the previous CRL. This update will reflect the removal of any superseded information. Copies of each CRL written to the repository are made to a separate location so that all CRLs will be archived. Additionally, CRLs (those both in the repository and those written to a separate location) are backed up nightly.

In the event of the CSOS CA certificate revocation, the DEA Bridge CA will post the revoked CSOS CA certificate to the ARL in the DEA Bridge CA repository. CSOS RA and Help Desk personnel will notify CSOS Coordinators of the CSOS CA revocation via a telephone call.

4.4.9.2 CRL Checking Requirements

The CSOS CA repository currently supports LDAP-accessible distributed, or partitioned, CRLs. The issuing CA's private key signs all CRLs.

CRLs may be cached and used until they expire unless otherwise notified by the PMA through the DEA E-Commerce Web site at, www.DEAecom.gov or email or phone call from the CSOS Help Desk to the CSOS Coordinators. CSOS Coordinators must perform a callback to the Help Desk to authenticate the message. In the event that an emergency or other incident prevents the CSOS CA from publishing a CRL, relying parties may rely on the cached CRL until another CRL is issued. The CSOS CA Help Desk will provide email notification to CSOS Coordinators when CRL services are restored after interruption.

The Relying Party's application software performs CRL checking of certificates at the time the certificate is validated, checking to ensure 1) the certificate was valid at the time of signing, 2) the Subscriber's certificate was signed by the CSOS CA, and 3) the CSOS CA's certificate is not present on the DEA Diversion Control E-Commerce System's Root CA's ARL.

CRL checking requirements associated with Relying Party acceptance of CSOS Subscriber certificates is specified in Title 21 CFR Part 1300.

4.4.9.3 On-line Revocation/Status Checking Availability

The CSOS CA does not support the Online Certificate Status Checking Protocol (OCSP) capability for its CRLs at this time.

4.4.9.4 On-line Revocation Checking Requirements

The CSOS CA does not support any forms of Online Revocation Checking at this time.

4.4.9.5 Other Forms of Revocation Advertisements Available

The CSOS CA does not support any other forms of revocation advertisements. Other forms of revocation advertisements will be reviewed for applicability on a periodic basis or as requested by the CSOS community.

4.4.9.6 Checking Requirements for Other Forms of Revocation

In the event that the DEA Diversion Control E-Commerce System Root CA or CSOS CA is unable to publish its revocation list as described in this CPS, the Help Desk will provide either a telephone call or digitally-signed email to all CSOS Coordinators with information on an alternative location of the CRL or DEA-authorized procedures for revocation checking. This notification will also be posted to the DEA web site at www.DEAecom.gov, accessible to all Relying Parties.

4.5 Security Audit Procedures

The following represents a sanitized description of CSOS security audit procedures. Information representing “critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities” has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.

The DEA Diversion Control E-Commerce System generates audit log files for events relating to the security of the CSOS CA. These audit logs consist of system logs, application logs, and hardware syslogs. Where possible, automatically generated audit logs are written to a protected log server and stored on media that prevents undetected log tampering. These logs are then provided to the Security Officer, who compiles and parses the logs – importing them into a database. Using automated tools and scripts that flag suspicious or high-risk events; the Security Officer performs a daily review of these security logs.

Where the automatic collection of logs is not possible (e.g., with visitor sign-ins), a logbook, paper form, or other physical mechanism is used (depending on the audited event.) All security logs (automatic or manual) are retained in accordance with Section 4.5.3, becoming part of the archive.

4.5.1 Types of Events Recorded

Security audit logging, as described below, is enabled for all events relating to the security of the CA. Where audit logs are not automatically collected, logbooks, paper form, or other physical mechanisms are used, depending on the audited event. All security audit logs, both electronic and non-electronic, are retained and made available during compliance audits. The security audit logs for each auditable event defined in this section are maintained in accordance with Section 4.5.3.

All significant CA security events are recorded in audit trail files. The audit trail files include the following elements:

- Type of entry;
- Date and time of entry;
- A success or failure indicator when executing the CA's signing process;
- A success or failure indicator when performing certificate revocation; and
- Identity of the entity and/or operator that caused the event.

A message from any source requesting an action by the CA is an auditable event; the message must include the message date and time, source, destination, and contents.

4.5.2 Frequency of Processing Log

Audit log reviews are performed on a daily basis by the Security Officer. All security alerts and irregularities are explained in an audit log summary. The Security Officer reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews are documented. In the event of a reported security incident, the Security Officer immediately reviews all appropriate audit logs.

4.5.3 Retention Period for Audit Log

Copies of the audit logs are retained onsite for at least two months to facilitate investigations and inquiries.

Audit logs retained as archive records are transported to the archive facility and are maintained for a period 10 years, 6 months.

The Security Officer or System Administrator removes the audit logs from the Diversion system and does not command the Diversion Root and CSOS CA signature key(s).

4.5.4 Protection of Audit Log

The following represents a sanitized description of audit log protections presently in place. Information representing "critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities" has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.

The Security Officer performs the daily review of security audit logs. Daily audit logs have a network-synchronized date and time associated with them, with labels carrying the date and time on which they were created. The logs are protected from deletion and/or modification prior to the end of the audit log retention period. See Sections 4.5.5, 4.5.6, 4.6, and 5.0 for additional descriptions of physical and procedural controls for protection of the data.

4.5.5 Audit Log Backup Procedures

Computer-generated audit logs and audit log summaries are backed up onto tamper-proof media on a daily basis. Manual audit records are stored in a secure container in the Diversion PKI facility. Audit log records are transported to the archive location monthly.

Full backups of the systems, including automatically collected audit logs, are performed weekly (e.g., on a fixed week day). Differential backups are performed daily.

All backups are stored in secure container in a separate building from the Diversion PKI facility.

Daily differential backups are securely erased and reused after three months – or destroyed depending on the media employed. Archived full volume backups are kept for at least 10 years, 6 months.

4.5.6 Audit Collection System

The automatic log collection systems are internal to the Diversion PKI Operating System and application components. Automated audit processes are invoked at system startup, and cease only at system shutdown.

4.5.7 Vulnerability Assessment

The Diversion PKI OMA and staff perform self-assessments of the security controls at the time of initial installation and configuration of the Diversion PKI components. Periodic vulnerability assessments are performed quarterly, upon notification of updates to vulnerability scanning

software signature files, or following a system configuration change with the potential for effecting system security (e.g., hardware, software, or network changes or upgrades).

The Security Officer performs additional vulnerability assessments as part of security compliance audits as specified by the Diversion PMA. The Diversion PKI OMA and staff provide a report of the analysis of the results of vulnerability assessments, specifically indicating security vulnerabilities identified and correction procedures of those vulnerabilities.

The Security Officer coordinates with the PKI Engineering team, utilizing network, database, and system scanning tools, monitoring CERT advisories and reviewing operating system and application patches, to identify potential vulnerabilities or events that would affect the integrity and operation of the CA.

4.6 CA Records Archival

4.6.1 Types of Events Recorded

At initialization, the Diversion PKI system equipment configuration files are archived, as well as the CPS and any contractual agreements to which the Diversion PKI OA is bound. During Diversion PKI operation, the following data are recorded for archive:

- Diversion PKI certification and accreditation, including any WebTrust Accreditation documents and DEA SSP documentation;
- Certification Policy and Practices Statement;
- Contractual obligations;
- System and equipment configuration;
- Modifications and updates to system or configuration;
- Certificate requests;
- Revocation requests;
- Subscriber identity authentication data;
- Documentation of receipt and acceptance of certificates;
- Documentation of receipt of tokens;
- All certificates issued or published;
- Record of Re-key;

- All CARLs and CRLs issued and/or published;
- All audit logs;
- Other data or applications to verify archive contents; and
- Documentation required by compliance security officers.

4.6.2 Retention Period for Archive

Archive of the certificate and audit trail information is retained and protected against modification and destruction for a period of at least 10 years, six months, exceeding DEA agency requirements. All applications resident on the system are backed up in full-volume backups and archived for 10 years, 6 months in order to recover or read the archived data.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media will be defined and approved by the OMA and PMA.

Prior to the end of the archive retention period, the OMA will provide the archived data and the applications necessary to read the archives to the PMA for Agency disposal.

4.6.3 Protection of Archive

The following processes ensure the protection and integrity of the CSOS archive:

- The media used to store audit logs and data have expected lifetimes exceeding the archive retention period requirements.
- Physical and logical access controls protect the archive. The Diversion PKI archive site is located in a facility separate from the primary facility.
- The archive facility is temperature controlled and behind locked computer room doors.
- The contents of the archive may be retrieved archive will not be released except as determined by the Diversion PKI PMA or as required by law.
- Only the Diversion PKI Security Officer is authorized to transport archive data to the archive facility.

4.6.4 Archive Backup Procedures

Two sets of full-volume weekly backups are performed each week. One set is stored off-site at the interim backup facility to use in the event that system or data recovery is necessary and is rotated every three months and one set is transported monthly to the archive facility.

These media will be clearly labeled with the Diversion DN and the date/time information and marked “For Official Use Only” in accordance with DEA guidelines. Full volume backups

containing RA database information, or paper records containing SSN information is additionally marked with the following label: “Warning: This Information Requires Protection Under the Privacy Act”.

Audit logs are archived as discussed in Section 4.5.4, labeled with the Diversion DN and date/time information and marked as discussed above. These archive media are securely stored off-site, as discussed in Section 4.6.3, until they are transported to the archive facility.

System Administrators verify backup integrity by viewing the backup logs for errors and then hand-carry the backups to the off-site location for short-term storage and subsequent transport to the archive facility.

Differential backups are performed daily and are stored at the backup facility for a two-week period. These differential backups are used for short-term restoration requirements and are not archived.

In the event that restoration of system or data is necessary, full-volume backups plus the latest differential backup are used to quickly restore the system to within 24 hours of the failure. Backup procedures are detailed in internal system documentation. Restoration procedures are detailed in a contingency plan internal to the system.

Archive data is clearly labeled for transport to the off-site backup and archive locations. The Security Officer will maintain logging information (and receipts) as archived data is transported from the backup facility to the archive facility. Transport of archive data is hand-carried to the archive facility by the Security Officer.

4.6.5 Requirements for Time-Stamping of Records

All CA archive records are automatically time-stamped as they are created. DEA maintains redundant connections to NIST’s clock that is then transmitted to the CA servers by an authoritative timeserver ensuring that all systems maintain synchronized time.

4.6.6 Archive Collection System

Records are clearly labeled with the Diversion PKI DN and date/time period information of the data contained in the record. The backup-labeling format is:

Diversion E-Commerce System - Network (RA/Private) - Media Type (Tape) - Backup Type (Full/Differential) - Location (On-Site/Off-Site) - Date (MM/DD/YYYY) - Tape Number out of Total (Number/Total).

Example: Diversion E-Commerce System - Private - Tape - Full - Off-Site - 01/01/2004 - 1/2

The media labeling format will be:

Diversion E-Commerce System - Media Type (DVD) - Backup Type (Full) - Location (On-Site/Off-Site) - Date (MM/DD/YYYY) - Tape Number out of Total (Number/Total).

Example: Diversion E-Commerce System - DVD - Full - On-Site - 01/01/2004 - 1/1

4.6.7 Procedures to Obtain and Verify Archive Information

Requests for archived Subscriber information from the Subscriber:

Subscribers may request archived information about their individual CSOS records. Records are retrievable by a personal identifier or by other appropriate type of designation approved by DEA and made available to CSOS PKI participants at the time of their application for CSOS PKI services. The DEA will make available to the CSOS PKI Subscribers all information it has collected following an appropriate request for information or correction if necessary. Instructions for requesting information are provided to Subscribers at www.DEAecom.gov and in the CSOS Privacy Policy on the CSOS Web site. Requests must be submitted, in writing, to:

Drug Enforcement Administration
Office of Diversion Control
E-Commerce Program (ODC)
Washington, DC 22202

Attn: Chief, E-Commerce Section

Under the Freedom of Information Act (FOIA), CSOS Subscribers may request information be amended. While this is unlikely to happen, the following discusses how a request to amend a CSOS record is processed. Requests for an amendment must include:

a) The name of the individual subscriber requesting the amendment,

b) A description of the item or items to be amended,

c) The specific reason for the amendment,

d) The type of amendment action sought (e.g., deletion, correction or addition), and

e) Copies of available documentary evidence supporting the request.

The Security Officer maintains a record of each request for amendment that it receives, including the date and time the request was received, the name of the record, and information provided in support of the request.

The Security Officer will provide to the requesting individual subscriber written or e-mail acknowledgment of the receipt of his/her request for amendment within ten (10) working days of the date of receipt of that request.

DEA will make any appropriate corrections to any record or portion thereof that are required to ensure that the record is accurate, relevant, timely, and/or complete, within twenty (20) working days of the date of receipt of a request for amendment of that record. A copy of the corrections made, if any, will be made a part of the record of the request for amendment and a copy of which will be forwarded to the CSOS RA, if applicable. Written or e-mail notification of the correction will also be provided within (10) days to any person or agency to whom that record was previously disclosed, and a copy of that notification will be made a part of the record. The CSOS Help Desk will notify the individual Subscriber making the request in writing or by e-mail of any amendments that are made to the record. A copy of the notification will be made a part of the record of the request for amendment.

Requests for archived information from other parties:

The contents of the archive will not be released except as determined by the Diversion PKI E-Commerce Section Chief or as required by law. Requests by law enforcement for Subscriber information are subject to the conditions specified in Section 2.8.2. The DEA will make available information it has collected following an appropriate written request for information. Requests must be submitted in writing to:

Drug Enforcement Administration
Office of Diversion Control
E-Commerce Program (ODC)
Washington, D.C. 22202

ATTN: Chief, E-Commerce Section

Procedures for retrieving archived data:

The E-Commerce Section Chief will approve the request and provide the information to be retrieved to the Security Officer, who will record the request and retrieve the data from the archive. The Security Officer maintains a record of each request for information that it receives, including the date and time the request was received, the name of the record, and information provided in support of the request.

The Security Officer maintains logging information (and receipts) for data retrieved from the archive. Archive records will be maintained under the control of the Security Officer, who will extract the requested data from the archived tape, paper record or CD, making copies of the information to be delivered to the PMA for delivery to the requestor, ensuring that original archive media does not leave the DEA archive facility or the CSOS CA and the control of the Security Officer.

The Security Officer will, on an annual basis, retrieve a sampling of data archived onto storage media and will restore the records onto the Test and Evaluation system to ensure that the records remain recoverable and have not become corrupted.

4.7 CA Key Changeover

The CSOS CA certificate and signing keys have a validity period of 6 years. The CSOS CA will generate a certificate request to the DEA E-Commerce System Root CA prior to less than 3 years remaining on the current key pair to allow for uninterrupted validity of all subjects. The key changeover procedure will be as follows:

- The CSOS CA will cease to issue new certificates no later than sixty (60) days before the point in time (“Stop Issuance Date”) when the remaining lifetime of the CSOS CA key pair equals 3 years.
- The CSOS CA will generate a certificate request with a new key pair, signed by the old private key.
- The certificate request will be transferred to the DEA Bridge CA (the "Root CA") on a floppy disk, where it will be signed by the Root CA and transferred back to the CSOS CA via floppy disk.
- New Subscriber certificate requests that are received after the “Stop Issuance Date" will be signed using the new CSOS CA key pair.
- The CSOS CA will continue to issue CRLs signed with the original CSOS CA private key until the expiration date of the last certificate issued using the original key pair has been reached.

All certificates generated, as part of the key changeover process will be posted to the CSOS repository.

4.8 Compromise and Disaster Recovery

4.8.1 Disaster Recovery

The following information is protected at the DEA archive facility:

- Backup CA private key and activation data
- CA database records, including issued CRLs and repository records
- Log files
- Scanned images of the Subscriber application packets
- Hard and electronic copies of security documentation
- Accounts and passwords necessary to access the restored system

A comprehensive contingency plan is in place that addresses potential disaster scenarios. The contingency, incident response, and key compromise plans vary according to the nature of

scenarios identified, however all detail the steps to be taken given a number of different events with the goal of providing 24/7 status checking services to the CSOS community. A summary of the steps that will be accomplished to regain system functionality follows:

1. Key personnel will be notified and activated. Notification information is located in a contingency plan at DEA. A notification list is maintained at the Help Desk and with the Security Officer. The Help Desk serves as the primary point of contact during a disaster, ensuring that key personnel are notified as directed in CSOS' contingency plan. Copies of the plan containing contact information and planned procedures are located in both the primary and secondary facilities, and operators receive regular training in their roles.

2. Based on the scenario, activation of recovery procedures for that situation and severity will be put into effect.

3. If the assessment of the event appears that capability will exceed 24 hours, or the event severity warrants, activation of the backup site will be put into effect. If possible, the backup site will use the same URL for CRL distribution. A warm backup site has been designated and contains sufficient duplicate equipment and a live communication link necessary to provide a 24-hour window for CSOS CA service re-activation.

4. If the backup site is unable to use the same CRL distribution URL, the Help Desk will notify CSOS Coordinators of the change or other DEA authorized provision for status checking via telephone notification.

5. The warm site is quickly restored via trusted images and backup media. CA Key restoration/activation on the restored CA system will be performed under the same two-person controls as was required with the primary CA system.

6. Upon system and CA restoration, the CARL and CRLs will be checked to ensure that they reflect the current certificate status. Any certificates generated that day that do not appear in the repository records will be manually revoked.

7. Post recovery audit logs will be submitted to the PMA for review. These logs will include all manual and automated event logs to demonstrate that security processes commensurate to the primary CA system have been applied during the restoration of services at the warm site.

The DEA Diversion Control E-Commerce System's contingency plan contains detailed information for multiple disaster scenarios.

The facility housing the CA operates with backup-up power and appropriate infrastructure system redundancies so no extended power outages are anticipated. In the event whereby the CA primary installation is physically damaged and all copies of the CA signature key are destroyed as a result, the PMA will be securely notified (via callback and challenge and response), and the alternate site placed into interim service until the primary facility can be completely rebuilt, re-certify, and can begin to generate new private and public keys.

4.8.2 Key Compromise Plan

In the event the CSOS CA private key is compromised, the CSOS CA will implement the DEA Diversion Control E-Commerce System key compromise plan. A summary of steps that will be followed include:

1. The CA will immediately revoke all of the certificates it has issued and its own certificate and will post its CRL in the repository and on DEA's Web site.

2. The CA will generate a new CSOS CA private key.

3. An RA script has been created that can be manually run in the event of key compromise. This script generates a listing of CSOS Coordinators and their Subscribers and sends a digitally signed email to all Subscribers via their CSOS Coordinators informing them that their certificates have been revoked and that they must obtain new certificates, providing them information on how they can re-enroll for new certificates.

4. The compromise will be investigated and reported to the PMA.

4.9 CA Termination

In the event of CSOS CA termination, the PMA will oversee the termination process. The CA Help Desk staff will work to notify all Subscribers and CSOS Coordinators of the CSOS CA cessation of operation via telephone call or digitally signed email. All certificates issued by the CSOS CA will be revoked. Prior to CA termination, all archived data will be provided to an archival facility under the supervision of the Security Officer and Operations Manager. Detailed internal system documentation describes the PMA's responsibilities during the termination process.

Section 5 – Physical, Procedural, and Personnel Security Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The following represents a sanitized version of the site location and construction specifics. Information representing "critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities" has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.

The DEA Diversion Control E-Commerce space is located in a secure facility. Access into the building is controlled and monitored. Visitors, maintenance, and janitorial staff require escort at all times by cleared personnel.

5.1.2 Physical Access

The following represents a sanitized version of the physical access specifications. Information representing "critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities" has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.

A variety of controls are in place to ensure that access is protected, including smart card and biometric access controls, as well as closed circuit television monitoring systems. Security personnel monitor access to the facility.

5.1.3 Physical Access Controls

The following represents a sanitized version of the physical access controls in place. Information representing "critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities" has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.

A variety of controls are in place to ensure that access is protected, including smart card and biometric access controls, as well as closed circuit television monitoring systems. Security personnel monitor access to the facility.

Access into all spaces requires a DEA/DOJ clearance. All visitor, vendor and employee access must be approved by the E-Commerce Security Officer prior to entry into the facility. External facility management/maintenance personnel require escorted access all times. Access into the CA Server room requires 2-person access.

The last Security Officer exiting the facility ensures all critical components are secured and completes an "end-of-the-day" checklist, ensuring that the safe and doors are secured and sensitive RA documents are safely stored. Operations are on-going 24 hours a day, 7 days per week in which multiple operations personnel are present. In the unforeseen event that all personnel must vacate the facility for an extended period of time, the Security Officer on duty will perform a security check of the facility, ensuring that only essential equipment is powered-on. A log is maintained in which personnel are required to initial at each check, initialing a sign-out sheet as the last person leaves the facility. This sign-out sheet indicates the date and time and contains an assertion that "all necessary physical protection mechanisms are in place and activated". These protection mechanisms include the cryptographic modules, the security containers, the physical security controls, and the environmental controls. Upon returning to the facility, the Security Officer will check the automatic logs upon returning to ensure that unauthorized entry did not occur during that period.

The DEA E-Commerce System maintains a monitored fireproof safe (with multiple combination compartments) for securing sensitive and confidential items. The safe has several compartments with secured containers (lockboxes) within it to separate and secure sensitive material.

Automatic logs are generated each time the CA private signing keys are activated and used.

An access policy is that details escort procedures for physical access is specified within the *Rules of Behavior* document and is provided to all new employees.

5.1.4 Environmental Controls

5.1.4.1 Fire Safety

The fire resistance of the primary location is high and the fire protection and suppression facilities available to the building are excellent, therefore the risk of substantial destruction as a result of fire of the equipment located in the building is deemed to be low.

There are two forms of fire suppression installed.

5.1.4.2 Water Exposure

The air-conditioning drip pans in the CA room contain electronic water bugs used indicate water leaks and is monitored. Two additional floor water sensors are planned to indicate water leaks accumulating on the floor.

5.1.4.3 Electrical Power

The following represents a sanitized version of the electrical power controls in place. Information representing "critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities" has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.

The commercial power system supply to the CA facility is extremely reliable. Outages are mitigated by the presence of an uninterrupted power source for the system that protects against power surges, spikes, and sags as well. Backup power sources are routinely tested.

5.1.4.4 Air Conditioning

The temperature in the CA room is maintained at 69+-2 degrees to enhance the life of the UPS batteries and CA equipment and is monitored 24x7 an independent vendor. There are multiple air-conditioning systems, each capable of supporting the temperature requirements alone. Temperature is appropriately maintained in the facility in the event of a power outage.

5.1.5 Cabling and Network Devices

Cabling and network components supporting CA services are stored in locked rooms, protected from interception and damage.

Access to the communication equipment is accessible only to Nortel Government Solutions, Inc. personnel and authorized maintenance personnel.

5.1.6 Storage Media Handling, Destruction, and Reuse

The E-Commerce facility includes a fireproof safe subject to two-person control that provides protection to sensitive media and devices. Media that contains audit or archive data is stored in a location separate from the E-Commerce facility until it is transported to a long-term storage site as specified in Section 4.6.2. Backup media and hard drives are returned to DEA for destruction. System storage media and devices containing storage media are overwritten using forensic utilities that permanently remove data from the media through performing a series of formats, at least three times, prior to reuse or destruction. Removable cryptographic modules are zeroized or re-initialized prior to destruction. When not in use, removable cryptographic modules, activation

information used to access or enable cryptographic modules, and CA equipment will be placed in the two-person controlled safe. Activation data is either memorized or recorded and stored in the safe. A separate secure container within the safe is used to secure the cryptographic module, separate from its activation data. Custodial personnel are allowed into the facility only when escorted by staff.

5.1.7 Off-site Backup

Full and interim (differential) system backups, sufficient to recover from total system failure, are conducted as described in this CPS and are located in a building that is separate from the primary facility. The backup facility possesses an independently operated HVAC and an UPS system sufficient to afford time for a graceful shutdown period. The room is physically secured through the use of the same card-key system present in the production facility. A locked safe in the off-site backup facility securely stores the backups. These components and their application to disaster recovery are described more fully in a contingency plan internal to the system. Long-term archived records are stored in a DEA-secured facility that is accessible only to DEA-cleared personnel.

5.2 Procedural Controls

Accurate procedures detailing roles, responsibilities, and tasks exist within internal system documentation to control setup, changes and use of equipment, software and operating procedures. Reporting and response procedures exist, detailing points of contact and actions to be taken in the event of security incidents and malfunctions. These documents reside in the CA Operations area and are made available to appropriate personnel.

5.2.1 Trusted Roles

To ensure that one person acting alone cannot circumvent safeguards, the responsibilities of the CA are shared among multiple individuals. Each account on the CA system will have limited capabilities commensurate with the individual’s role. The trusted roles within the CA are:

5.2.1.1 Shareholders

Shareholders do not hold an account on any of the systems and have been provided with the tokens that are required for any task involving activation of the CA’s private signing key.

5.2.1.2 CA Operators

CA Operators are defined, within this PKI, as personnel trained in the operation of the CA and who are responsible for key management. At least two individuals with CA Operator rights will perform the role of CA Operator at any one time. In addition to facility access controls that require at least two individuals be present in the CA room, the CA application has been configured such that two-person authentication at the CA is enforced for sensitive CA operations.

The CA Operators have the authority and access to:

- Set and modify the CA security policy, in accordance with this CPS and the CP;
- Generate applicant access codes and passwords;
- Administer the CA repository;
- Process the file sent to them electronically from the RA that issues or revokes certificates;
- Add and remove other CA Operators;
- Issue CRLs;
- Review CA audit logs.

5.2.1.3 Registration Authority Operators and Staff

RA support personnel have the overall responsibility for adjudicating DEA Diversion Control applicants. RA responsibilities include:

- Reviewing applicant information for validity;
- Approving or denying an applicant's request for a CSOS Certificate;
- Requesting for generation of enrollment access codes and passwords;
- Supplying an applicant with information deemed necessary to interact with the CSOS PKI;
- Creating the file authorizing certificate issuance or revocation and distributing the file to the CA;
- Informing applicants of any request or status of request as necessary.

5.2.1.4 Security Officers

The Security Manager and staff serve as Security Officers and have the overall responsibility for ensuring that all security procedures are carried out. The CA Security Officers are responsible for:

- Setting the number of required authorizations for sensitive operations;
- Reviewing audit logs;
- Enforcing the CSOS information security configuration and monitor the user access process to ensure operational integrity of the system;
- Reporting security violations, any attempts to gain unauthorized access to information, virus infection, or any other event affecting the security of the E-Commerce CA to the appropriate parties described in the incident response plan;
- Overseeing the sanitization of media containing sensitive information prior to release;
- Performing periodic risk and vulnerability assessments;

- Performing secure storage and distribution of backups and upgrades to an offsite location;
- Performing periodic security audits;
- Daily examination of the system security reports for suspicious activity;
- IDS monitoring and firewall alert monitoring;
- Archival of security data;
- Incident response handling;
- Forensic protection;
- Continually monitoring Computer Emergency Response Team (CERT) advisories for new vulnerabilities that may affect the security of the DEA Diversion Control PKI;
- Assisting with the investigation and report writing for security incidents;
- Ensuring that the password management system is implemented and enforced;
- Providing guidance to DEA Diversion Control PKI personnel pertaining to the labeling of sensitive documents and files;
- Overseeing, enforcing and testing the physical security measures, including physical access and environmental controls.

5.2.1.5 System Administrators

System Administrators are assigned the overall responsibility to ensure that the DEA Diversion Control E-Commerce systems are operational. System Administrators do not issue or manage certificates to Subscribers. The CA System Administrators responsibilities include:

- Configuration of the DEA Diversion Control PKI platform, to include application installation, account setup and host and network interface configuration and modification, as provided in instructions received from the Engineering team under the Configuration Control Board's governance;
- Configuring systems to support recovery from catastrophic system loss, performing system backups, software upgrades and recovery;
- Validating backup integrity;
- Verifying the removal of all default accounts after any software installation;
- Implementing controls that ensure that password management policies are enforced;
- Daily monitoring and management of system and user activity;
- Responding to all notifications of unauthorized actions on accounts, files and directories, and unauthorized connections to/from the DEA Diversion Control PKI platform, notifying the Security Officer of such an event.

5.2.1.6 Help Desk Staff

The CSOS Help Desk is a part of the CSOS RA function as specified in Section 5.2.1.3 above and, as such, is considered to be a trusted role. Help Desk support personnel have the overall responsibility for serving as the interface between the CSOS User Community and CSOS Operations Staff. Help Desk responsibilities include:

- Answering telephone inquiries for CSOS Information;
- Authenticating and processing revocation requests;
- Escalating and forwarding calls to appropriate Operations Staff;
- Serving as the single point of contact for Engineering and Operations Staff notification during disaster recovery, key compromise, or in the event of an incident response.
- Assisting CSOS Subscribers with problems encountered during downloading Subscriber certificates.
- Provide notification to CSOS Subscribers and Coordinators in the event of key compromise.

5.2.2 Separation of Roles

The following contains a sanitized description of CSOS role separation. Information representing "critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities" has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties. Role separation, as described below, is enforced by operating system or application software controls or procedurally, or by both means.

Individual CA personnel are assigned a single unique user accounts and are then assigned to only one of the roles defined Section 5.2.1 above.

To ensure the integrity of the DEA Diversion PKI CA equipment and operation, the security policy requires two persons to authorize or perform sensitive operations. The complete CPS details these controls and is available upon request as detailed in Section 1.1.

5.2.3 Identification and Authentication for Each Role

All personnel must provide their unique user account and password to identify and authenticate themselves to the system before accessing any application, including those involved in trusted roles (as with the CA application). All PKI personnel are provided role membership that limits their activities to the duties and responsibilities described in the sections above. The Security Officer has been assigned the responsibility of periodically reviewing user access rights and, as

stated above, performs periodic vulnerability assessments to ensure that password policies, as defined in the *Rules of Behavior* document, is strictly adhered to.

5.3 Personnel Controls

5.3.1 Personnel Security Controls for Certification Authority

At least three individuals are to be assigned Shareholder responsibility at all times. If one of these positions is vacant, the OMA will nominate a temporary replacement.

At least two individuals are assigned CA Operator privileges at any one time.

All DEA Diversion Control E-Commerce System personnel undergo background investigations and are hired only after references are validated and DEA Security clearances are obtained.

CA personnel are hired specifically to serve in their designated role and have completed appropriate training and are familiar with CSOS system documentation.

5.3.2 Background Check Procedures

All CA personnel are required to undergo a DEA Sensitive background investigation. All background checks are performed by DEA in accordance with DEA Personnel Security Policies and are performed at the time an offer is extended to the applicant. Positions are contingent on DEA acceptance and successful clearance adjudication. All CA personnel are U.S. Citizens.

5.3.3 Training Requirements

A comprehensive training plan details the Security and Operational training, by role, required of personnel. The Security Officer is designated with the responsibility to manage individual employee training plans. This training includes:

- Initial Security Training Briefings/Rules of Behavior Training;
- Training in the operation of the software and/or hardware used in the E-Commerce System;
- Training in the duties personnel are expected to perform e.g., contingency plan;
- Briefing on relevant details of this CPS and the CP;
- Ongoing training in security procedures and policies, including disaster recovery and incident response.

5.3.4 Retraining Frequency and Requirements

Any significant change to the operations is documented and personnel are informed and made aware of changes. Training is provided to affected personnel whenever system changes are made.

Security training is required on an annual basis for all employees. The DEA Diversion Control E-Commerce Security Officer is assigned the responsibility for tracking personnel training requirements.

5.3.5 Sanctions For Unauthorized Actions

In the event of an actual or suspected unauthorized action by a person performing duties that support the DEA E-Commerce system, the E-Commerce Section Chief will be notified via the Operations Manager or Security Officer. The E-Commerce Section Chief or Operations Manager may suspend his or her access to the E-Commerce system and/or E-Commerce facility.

Breach of this CPS or the CP whether through negligence or through malicious intent, is subject to privilege revocation, administrative discipline, and/or criminal prosecution.

5.3.6 Employee Termination Controls

Once an employee terminates employment, or is terminated, the Security Officer will ensure that all physical or technical access controls are revoked or disabled immediately upon notification from the Operations Manager. The Security Officer will note the time and date of account access termination and revocation of any issued administrative certificates or physical access on the employee's account paperwork and will archive this information in accordance with other security-relevant documentation.

5.3.7 Contracting Personnel

Contractor personnel employed operating any part of the DEA Diversion Control E-Commerce System meet all applicable requirements set forth in the CP or this CPS and are cleared to the level of the role performed as identified in Section 5.3.1.

5.3.8 Documentation Supplied To Personnel

This CPS, the CP, and all relevant security documentation are made available to DEA E-Commerce personnel. New employees are provided with, and briefed on, the *Rules of Behavior* document that specifies acceptable use of the system, the facility access policies, and other system requirements. Operations manuals are made available to personnel to facilitate the operation and maintenance of the systems hardware and software.

DEA Sensitive documentation is marked accordingly on the front of the documentation and securely stored in locked drawers or file cabinets when not in use. Working documentation and deliverables are stored in VSS, protected with access controls to ensure that only authorized personnel have access to them. All documentation changes adhere to processes defined in a configuration management plan.

5.3.9 Personnel Security Controls for End Entities

Subscribers are provided with information on the use and protection of the software used within the CSOS system in a CSOS Subscriber's Manual located on the CSOS Web site. A Questions and Answers page is present on the Web site that addresses many commonly asked questions. Additionally, Subscribers are directed to contact the CSOS Help Desk for technical assistance.

Section 6 – Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The CSOS CA digital signature key pairs are generated on the cryptographic module during the initial installation of the CA application under 2-person control enforced within the O/S login procedures and CA application software.

The CSOS CA key pair was generated in a pre-planned Key Generation, witnessed by KPMG and DEA personnel. The activities performed in each key generation ceremony are scripted, dated and signed all individuals involved in the ceremony. These records are kept for audit and tracking purposes for 10 years, 6 months beyond the date of the last certificate issued by the system.

Key pair generation is RSA 2048 for digital signature in compliance with PKCS-1 (FIPS 140-1, level 3. Practice note: FIPS 140-2 grandfathers products certified at FIPS 140-1).

The private keys are never exposed outside of the modules in unencrypted form.

Backup copies of the cryptographic module are created during key generation and are securely stored both at onsite and offsite locations.

6.1.2 Private Key Delivery to Entity

No private keys are exchanged between the CA and any entity. Subscribers generate their own private keys.

6.1.3 Public Key Delivery to Certificate Issuer

Delivery of the public key from the Subscriber to the CSOS CA is electronically secured using SSL with 128-bit encryption and requires proof-of-possession (PoP) using an Initial Authentication Key (IAK) and Reference Value (auth and ref codes) that are distributed to the Subscriber in an out-of-band procedure, consistent with IETF RFC 2510.

6.1.4 CA Public Key Delivery to Users

The public key of the CSOS CA signing key pair is delivered to Subscribers in an SSL-secured online transaction in accordance with IETF PKIX Part 3, PKCS 7. Instructions are provided to the Subscriber in the CSOS Subscriber’s Guide on how to validate the hash of the CA public key imported from the CSOS Web site.

6.1.5 Key Sizes and Algorithms

The CA digital signature key pair is 2048-bit RSA Secure Hash Algorithm version 1 (SHA-1) in accordance with FIPS 186-2.

SHA-256 will be used for Subscriber keys that are issued after 12/31/08.

The key pair used for SSL is 1024-bit RSA.

Subscriber keys are 1024-bit RSA. Subscriber certificates that are used for signing on or after January 1, 2009 will contain public keys that are at least 2048 bit-RSA, in accordance with FIPS 186-2.

6.1.6 Public Key Parameters Generation

There are no public key parameters for RSA.

6.1.7 Parameter Quality Checking

There are no public key parameters for RSA.

6.1.8 Hardware/Software Key Generation

The CSOS CA digital signature key pairs are generated in a FIPS 140-1 Level 3 validated, hardware cryptographic module (reference practice note in Section 6.1.1).

6.1.9 Key Usage Purposes (as per X.509 v3 key usage field)

CA keys are certified for use in a combination of Certificate Signing, Off-line CRL Signing, and CRL Signing in accordance with the *DEA Diversion Control E-Commerce System Certificate and CRL Profile.*

6.2. Private Key Protection

CSOS Subscriber certificates are to be used for signing purposes only. Subscriber private keys must not be backed up or escrowed. CA private keys may be backed up as specified below, however must not be escrowed.

The following sections describe the technical and procedural techniques for CA private key protection.

6.2.1 Standards for Cryptographic Module

The CA private key is protected using a FIPS 140-1 Level 3 validated cryptographic module.

Key pairs for CSOS CA activation are generated in a FIPS 140-1 Level 2 validated cryptographic module and all cryptographic modules are operated such that the private asymmetric cryptographic keys are never output in plaintext.

6.2.2 Private Key Multi-Person Control

All CA private keys are under 2 out of N control, where N is greater or equal to 2.

6.2.3 Private Key Escrow

The DEA Bridge CA's and CSOS CA's private keys are not escrowed.

6.2.3 Private Key Backup

The CA's private digital signature key is backed up under multi-person control on a token using a hardware device that is FIPS 140-1 Level 3 compliant. Multiple copies are maintained at geographically separate locations. Two backup copies are maintained and security stored. Text removed. Information representing "critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities" has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.

Access to those devices must only occur with at least two persons present.

6.2.4 Private Key Archival

No CA private keys will be archived.

6.2.5 Private Key Entry into Cryptographic Module

The CSOS CA's private digital signature key is generated in hardware within the cryptographic module that is FIPS 140-1 level 3 compliant under two-person control. The cryptographic module product uses proprietary secure means for transferring keys from one cryptographic module to another in order to back up the CA keys. The private key is only decrypted at the time of use.

6.2.6 Method of Activating Private Key

Activation of the CA private signing key is controlled under multi-person control, requiring two authorized personnel to perform key activation. Text removed. Information representing "critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those

facilities" has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.

6.2.7 Method of Deactivating Private Key

The CA's cryptographic module will be deactivated and stored in a secure container when not in use. Text removed. Information representing "critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities" has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.

6.2.8 Method of Destroying Private Key

Permanent destruction of the CA private digital signature key will be achieved by reinitializing/zeroizing the media the private key is stored upon under multi-person control. Destroyed keys are then provided to the DEA COTR for physical destruction at DEA's facility. Procedures for destroying the private key and reinitializing are detailed in internal system documentation.

PMA acceptance of this CPS indicates acceptance of this method.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The CA's verification public key certificate will be backed up with the CA database. The complete verification public key history for all Subscribers, including a history of status changes such as revocation date and reason, is also archived as a part of the certificate history archive.

6.3.2 Usage Periods for the Public and Private Keys

The CSOS CA private signing keys will be used to sign certificates for not more than one-half of the certificate lifetime (3 years). The CSOS CA private signing keys will continue to sign CRLs for the entire usage period (6 years). The certificate lifetime of the CSOS CA will be valid for not more than 6 years.

Subscriber private signing keys expire upon the expiration of the Subscriber's DEA registration, not to exceed 3 years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Text removed. Information representing "critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities" has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.

Once the CSOS CA private signing key is activated, use of the private signing key requires two-person control and is enforced by the CA application. Passwords used as activation data when accessing the CA application complies with FIPS 112.

6.4.2 Activation Data Protection

Activation data is protected by multi-person control, locked in secure containers to which no one person has access to both combinations and keys.

Text removed. Information representing "critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities" has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.

6.4.3 Other Aspects of Activation Data

Passwords are changed periodically, in compliance with password policies specified in the ***Rules of Behavior*** document, to decrease the likelihood of compromise.

Text removed. Information representing "critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities" has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.

6.5 CA Computer Security Controls

The CA server will be physically secured as described in Section 5.1 of this CPS and as specified in security documentation. Specific CA security controls include:

- The CSOS repository is operated on dedicated servers.
- Login requires FIPS 140-1, Level 3 cryptographic modules.
- Restricted access control to CA services and PKI roles, and enforced separation of duties of PKI roles and identities, as described in Section 5, within the CA application.
- Discretionary Access Controls are provided via permissions and policies defined in the CA software.
- All CA activity is automatically audited.
- Prohibits object re-use in CA random access memory.
- CA history and audit data is collected and archived as described in Sections 4.5.and 4.6.

Text removed. Information representing "critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities" has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.

6.6 Life Cycle Technical Controls

The CA cryptographic hardware installation requires a minimum of two trusted employees throughout its life cycle – from installation or key generation through key destruction.

6.6.1 System Development Controls

The following represents a sanitized version of system development controls in place for CSOS. Information representing "critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities" has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.

CA Equipment Purchases: The CA software is commercial-off-the-shelf (COTS) software that has been developed under a very formal development process that is well documented and evaluated by the vendor. All software and hardware installed on the DEA E-Commerce System has been purchased using commercial buys from U.S. vendors through appropriate DEA procurement channels whereby the provider does not know the intended purpose. Hardware and software updates will be purchased or developed in the same manner as the original equipment.

Software/Script Development Controls: Scripts developed for the RA and CA systems are managed such that access and modifications are limited and tracked.

Equipment/Software Receipt: An accountable method of packaging and delivery has been used to provide a continuous chain of accountability from the vendor to DEA, to the facility (e.g., UPS, Federal Express, USPS Express Mail). All software and hardware, from the time received, remains under continuous control.

Equipment/Software Installation: The Engineering team maintains test suites that are used to ensure that all devices and software used for private key storage and recovery and the interfaces to these devices are integrity tested prior to installation. Test results are documented and supplied to the Operations Team with the Build documentation. All software is scanned by anti-virus software prior to installation on DEA E-Commerce systems. Vulnerability assessments and a risk assessment are performed, depending on the changes made to the system, using a variety of vulnerability assessment tools. Vulnerability assessments that may impact performance, such as system scans are performed during off-peak hours.

Equipment Maintenance: Equipment maintenance is performed in accordance with the manufacturer's instructions to ensure its continued availability and integrity and that the CA continues to correctly process certificate requests. Diagnostic support at the CA, either by DEA CA or vendor personnel, is performed under two-person control. Other procedures, defined in internal system documentation, may be used for site-specific requirements.

Equipment Repair: Equipment repair is performed at the manufacturer's site. An accountable method of packaging and delivery to the vendor is used that provides a chain of accountability from DEA to the vendor's facility. A process exists for ensuring that inventory records are updated to reflect current location status. The removal of the cryptographic tokens from the hardware in the event that the PED or other CA equipment needs servicing or replaced with new hardware, firmware, or software is performed in the presence of no less than two trusted employees – storing the tokens in a safe subject to two-person access controls.

CA System Updates: Procedures for changes to be implemented on operational systems must be approved by a Configuration Control Board (CCB) and are documented in internal system documentation. Proposed changes and updates require the consideration of potential risks and are prioritized based on the identification of risk or efficiency-based factors.

All changes are tested in the test facility and are documented prior to installation on the production system. The production system is physically and logically separate from test and evaluation system. New hardware and software will be tested on a separate platform prior to implementation into the production platform for functionality, interoperability and vulnerabilities.

Patches and emergency software fixes are also tested on a separate platform prior to implementation to ensure functionality and to expose new vulnerabilities that may be introduced by their implementation. Procedures for implementation on operational systems are developed

during testing and are provided to Operations personnel with the updates. Copies of these documents are stored off-site. Trusted personnel responsible for implementing changes on the production systems receive appropriate training provided by the development team prior to implementation.

CA Equipment Destruction: When removed permanently from use, all DEA equipment and tamper-evident cases are provided to the DEA COTR in an accountable manner for destruction at the DEA Headquarters. Permanent destruction of the CA cryptographic modules is discussed in Section 6.2.8.

6.6.2 Security Management Controls

The initial configuration of the CA and supporting systems hardware and software (e.g., repository routers, firewalls, intrusion detection software) as well as any modifications and upgrades, is documented and controlled through change management processes defined in internal system documentation. System logging and auditing is reviewed daily to maintain the integrity of the software and approved configuration. All changes to the initial configuration are evaluated and approved by a CCB prior to implementation.

A security plan exists that details the security controls in place to ensure the secure operation of the CA and the integrity of its operating environment. The Security Officer is responsible for implementing and maintaining security documentation.

6.7 Network Security Controls

The following represents a sanitized version of the network security controls in place for CSOS. Information representing “critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities” has been removed in this publicly available version of the document and is, therefore, in compliance with the Federal Information Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a), §3544(A)(1)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3544(f). Upon request, the complete CPS document is available to authorized parties.

The public repository is connected to the Internet to provide continuous availability to the CSOS community. The repository is protected behind a firewall. External threats are mitigated by controls such as firewalls, network intrusion detection systems and router access lists to protect the network. A security plan exists that details the protocols allowed through the firewall to support the operation and interoperability of the repository.

Users are provided access only to services that they are specifically authorized to use from workstations designated for that function. Attempts to connect unauthorized workstations, laptops, or other devices to the network results are not permitted. Auditing policies have been implemented to mitigate both external and internal threats.

6.8 Cryptographic Module Engineering Controls

The CA cryptographic module is FIPS 140-1 Level 3 certified.

Section 7 – Certificate And CRL Profiles

7.1 Certificate Profile

The CSOS CA issues X.509 version 3 certificates in accordance with the *DEA E-Commerce System Certificate and CRL Profile*.

The CSOS CA uses the following fields of the X.509 version 3 certificate format:

- **Version:** version field is set to v3
- **Serial number:** when a new certificate is created, a unique serial number within the CA security domain is generated by the CA
- **Signature:** identifier for the algorithm used by the CA to sign the certificate.
- **Issuer:** CA Distinguished Name
- **Validity:** certificate validity period – the notBefore start date and notAfter end date are specified
- **Subject:** certificate subject distinguished name
- **Subject public key information:** includes the signing algorithm identifier and public key
- **Extensions:** see Section 7.1.2 below

The following fields of the X.509 version 3-certificate format are not used in this PKI:

- issuer unique identifier
- subject unique identifier

7.1.1 Version Number(s)

The CSOS CA issues X.509v3 certificates.

7.1.2 Certificate Extensions

A number of X.509 version 3 certificate extensions are included in certificates issued by this CA as well as two private extensions defined by this CA. These are outlined below. The X.509 version 3 certificate extensions, which are not present in certificates issued by this CA, are also outlined below.

The following certificate extensions are used in this CA:

X.509 v3 Certificate Extension	Critical/Non Critical	Required/ Optional	Notes
AuthorityKeyIdentifier	Non critical	Optional	Used where user may have multiple keys for signing. Identifies which key is used
SubjectKeyIdentifier	Non critical	Required	For chain building, and identifying certificates that contain a particular public key
BasicConstraints	Critical	Required	cA Boolean equals true
CRLDistributionPoints	Non critical	Optional	only 1 distribution point name is included in each certificate only element [0] (distributionPoint) is used and includes the full DN
KeyUsage	Critical	Required	Restricts how keys may be used. A subset of the following must be present: digitalSignature(required), NonRepudiation (optional), KeyCertSign (optional), and/or CRLSign (optional).
CertificatePolicies	Critical	Required	Indicates the policies under which the certificate has been issued.
EntrustVersionInfo	Non critical	Required	Certificate extension representing Entrust version
PrivateKeyUsagePeriod	Non critical	Required	This extension indicates the period of use of the private key corresponding to the certified public key
AuthorityInfoAccessSyntax	Non Critical	Optional	Used for non-CRL revocation methods
ExtKeyUsageSyntax	Non Critical	Optional	Extendable uses of public key, in addition to key usage

The following X.509 version 3 certificate extensions are not used in this CA:

- policy mappings
- name constraints
- policy constraints
- issuer alternative name
- subject directory attributes
- subject alternative name

7.1.3 Algorithm Object Identifiers

Algorithm	Object Identifier	Issuing Authority
Sha1WithRSAEncryption	1 2 840 113549 1 1 5	RSADSI

7.1.4 Name Forms

Every DN must be in the form of an X.501 **printableString.**

7.1.5 Name Constraints

Subject and Issuer DNs must comply with CSOS standards and be present in all certificates.

7.1.6 Certificate Policy Object Identifier

This CPS supports the CSOS Certificate Policy. This certificate policy applies to public key certificates issued for digital signature applications.

7.1.7 Usage of Policy Constraints Extension

The CSOS CA does not use policy constraints.

7.1.8 Policy Qualifiers Syntax and Semantics

CSOS Subscriber certificates have the policyQualifier extension populated with an explicit text notice as follows:

This is a DEA CSOS Digital Certificate. It is specifically intended for use in signing controlled substance orders - any other signing uses are at the discretion of the certificate holder.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

CSOS CA certificates under this policy will mark the certificate policy extension as critical. Critical extensions will be interpreted as defined in the IETF RFC 2459.

CRL Profile

The following fields of the X.509 version 2 CRL format are used in this CA:

- **Version:** set to v2
- **Signature:** identifier of the algorithm used to sign the CRL
- **Issuer:** the full Distinguished Name of the CA
- **This update:** time of CRL issuance

- **Next update:** time of next expected CRL update
- **Revoked certificates:** list of revoked certificate information

7.1.10 Version Number(s)

The CSOS CA will issue X.509 version 2 CRLs in accordance with the *DEA E-Commerce Certificate and CRL Profile.*

7.1.11 CRL and CRL Entry Extensions

A number of X.509 version 2 CRL and CRL entry extensions that are used in this PKI is outlined below. The X.509 version 2 CRL and CRL entry extensions that are never present in CRLs issued by this CA are also outlined below. The following exhibit identifies the CRL and CRL entry extensions that are used in this CA:

X.509 v2 CRL Extension	Critical/Non Critical	Required/ Optional	Notes
authorityKeyIdentifier	Non critical	Required	only element [0] (authorityKeyIdentifier) is filled in contains a 20 byte hash of the subjectPublicKeyInfo in the CA certificate
CRLNumber	Non critical	Required	Incremented each time a particular CRL/ARL is changed
deltaCRLIndicator	Critical	Optional	Improves processing time for applications that store revocation info. in a format other than the CRL
issuingDistributionPoint	Critical	Required	element [0] (distributionPoint) includes the full DN of the distribution point element [1] (onlyContainsUserCerts) is included for CRLs element [2] (onlyContainCACerts) is included for ARLs element [1] and [2] are never present together in the same revocation list elements [3] and [4] are not used
ReasonCode	Non critical	Required	CRL entry extension - supports all reason codes
holdInstructionCode	Non critical	Optional	CRL entry extension
InvalidityDate	Non critical	Required	CRL entry extension
certificateIssuer	Critical	Required	CRL entry extension

Exhibit 7-1. CRL and CRL Entry Extensions

The following X.509 version 2 CRL extension is not used in this CA: Issuer alternative name.

Section 8 – Specification Administration

8.1 Specification Change Procedures

The PMA will submit for processing any recommended changes communicated to the contact identified in Section 1.4. Updates to this CPS may be proposed at any time, however the OMA will submit all draft changes to the PMA for approval before incorporation into the CPS.

8.2 Publication and Notification Policies

Changes to items within this CPS, which will have no or minimal impact on the Subscriber using certificates and CRLs issued by this CSOS CA, may be made with no change to the CPS version number.

Changes to the certificates supported by this CPS as well as changes to items within this CPS which may have significant impact on the Subscriber using certificates and CRLs issued by this CSOS CA, will be made with 30 days notice to the user community, and the version number of this CPS must be increased accordingly.

8.3 CPS Approval Procedures

This initial CPS and all subsequent changes to the CPS will be formally approved by the PMA. The PMA must vote on the approval.